НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Теплоенергетичний факультет

Кафедра автоматизації проектування енергетичних процесів і систем

До захисту допущено:

Завідувач кафедри

_____ Олександр Коваль

«___»_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційні технології моніторингу довкілля»

спеціальності 122 «Комп'ютерні науки та інформаційні технології»
на тему:

«Реалізація використання блокчейн-технологій у енергетичному секторі»

Виконав: студент 4 курсу, групи ТМ-62

Євгеній ЛОКОТАРЬОВ _____
(ім'я, прізвище) (підпис)

Керівник к.е.н., доцент Ірина СЕГЕДА _____
(посада, вчене звання, науковий ступінь, ім'я, прізвище) (підпис)

Рецензент д.т.н., професор завідувач кафедри ТПТ Геннадій ВАРЛАМОВ _____
(посада, вчене звання, науковий ступінь, ім'я, прізвище) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”

Факультет теплоенергетичний

Кафедра автоматизації проектування енергетичних процесів і систем

Рівень вищої освіти перший рівень

Напрям підготовки 122 Комп’ютерні науки та інформаційні технології

Спеціалізація Інформаційні технології моніторингу довкілля

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Олександр Коваль
(підпис)
”___”_____2020р.

ЗАВДАННЯ
на дипломну роботу студенту
Локотарьову Євгенію Олександровичу
(прізвище, ім’я, по батькові)

1. Тема роботи Реалізація використання блокчейн-технологій у енергетичному секторі

керівник роботи к.е.н., доцент Ірина СЕГЕДА
(науковий ступінь, вчене звання, ім’я, прізвище)

затверджена наказом вищого навчального закладу від ”25” травня 2020р. № **1168-с**
2. Строк подання студентом роботи ”10” червня 2019р.
3. Вихідні дані до роботи: мова програмування — Java, середовище розробки — Intellij Idea, середовище побудови діаграм — Microsoft Visio
4. Зміст розрахунково-пояснювальної записки (перелік завдань, які потрібно розробити) провести глибокий аналіз предметної області та можливості у використанні технології, ознайомитися з алгоритмами які використовуються з даною технологією, спроектувати прототип, спроектувати архітектуру системи, зробити висновки за результатами роботи
5. Перелік ілюстративного матеріалу:1. Автоматизована система з обліку та продажу енергоресурсів на основі блокчейну. 2. Діаграма прецедентів. 3. Приклад мережі. 4. Алгоритм створення транзакції. 5. Алгоритм оновлення блокчейну від початку вибору транзакції до внесення нового блоку в ланцюг. 5. Діаграма класів. 6. Засоби розробки. 7. Сторінка авторизації та реєстрації. 8. Сторінка транзакцій. 9. Сторінка створення транзакції. 10. Приклад репліки блокчейну

6. Дата видачі завдання «11» жовтня 2019 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітки
1.	Вивчення та аналіз задачі	12.02.2020 – 18.03.2020	
2	Розробка архітектури та загальної структури системи	27.03.2020 – 03.04.2020	
3.	Розробка структур окремих підсистем	09.04.2020 – 12.04.2020	
4.	Програмна реалізація системи	13.04.2020 – 17.05.2020	
5.	Оформлення пояснювальної записки	19.05.2020 – 04.06.2020	
6.	Захист програмного продукту	18.05.2020	
7.	Передзахист	1.06.2020 – 05.06.2020	
8.	Захист	15.06.2020 – 19.06.2020	

Студент _____ Євгеній ЛОКОТАРЬОВ
(підпис) (прізвище та ініціали,)

Керівник роботи _____ Ірина СЕГЕДА
(підпис) (прізвище та ініціали,)

АНОТАЦІЯ

В даній роботі приведено дослідження блокчейн-технологій з можливістю подальшого впровадження в енергетичній сфері. Описано алгоритми роботи блокчейну, обґрунтування обраних технологій та архітектура системи, що проектується. В роботі також показано процес роботи блокчейну в створеній системі.

Результатом апробації даної роботи є стаття в науковому журналі.

Записка містить 37 сторінок, 12 рисунків, 3 таблиці, 5 додатків і 45 бібліографічних найменувань за переліком посилань.

Ключові слова: блокчейн, алгоритми хешування, блок, транзакція, майнинг, смарт-контракт, однорангова децентралізована система.

ABSTRACT

This work contains the blockchain’s technology research with an ability to be delivered in the power engineering further. The blockchain’s algorithms, chosen technology stack rationale and delivering system’s architecture are described. The blockhain’s flow in the developed system is also represented.

As a result of this work, a research article has already been published.

The note contains 37 pages, 12 figures 3 tables, 5 attachments and 45 links.

Keywords: blockchain, hashing algorithm, block, transaction, mining, smart-contract, peer-to-peer decentralized system.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Blockchain (блокчейн) — архітектурна концепція збереження інформації у формі блоків, пов’язаних один із одним.

Block — одиниця блокчейну, яка включає в собі набір транзакцій.

Transaction — одиниця блоку, яка зберігає корисну інформацію.

Smart contract (розумний контракт) — інформаційна одиниця, яка зберігає в собі дані про домовленості між сторонами.

Mining (майнинг) — процес обчислення хеш-значення методом перебору з метою доведення іншим користувачам, що не було проведено підробки даних.

Public key (публічний ключ) — криптографічне цифрове значення, доступне всім користувачам. В термінах блокчейну являє собою номер гаманця, на який необхідно переводити цифрову валюту, або, у випадку смарт-контрактів, адреса сторони, яка зафіксувала домовленість.

Private key (приватний ключ) — криптографічне цифрове значення, доступне лише власнику. За допомогою приватного ключа здійснюється цифровий підпис транзакції.

Peer-to-peer system (однорангова система) — архітектурна концепція інформаційних систем, де кожен із користувачів має один і той же рівень доступу до даних.

REST (Representational state transfer) — архітектурна концепція передачі даних.

MongoDB — нереляційна база даних, зі слабко вираженими зв’язками між даними.

ВСТУП

Розглядаючи наявні автоматизовані системи з обліку та торгівлі енергоресурсів, виникає питання у наявності додаткової вартості енергоресурсів за рахунок посередників, які забезпечують підтримку систем обліку та сплати енергоресурсів. Інше питання – неможливість здійснювати облік та оплату з одного, консолідованого додатку. Концепція обліку енергоресурсів з їх оплатою одночасно з цим стикується з інтернетом речей, де додаток буде мати можливість підключатися до «розумних» пристроїв, зчитувати з них інформацію, здійснювати контроль.

Мета даної роботи полягає в проектуванні спочатку прототипу, а потім і повноцінної автоматизованої системи, яка змогла би змінити поточний стан у ринку енергоресурсів України. Система, що проектується, базується на блокчейн технології і при впровадженні здатна організувати однорангову взаємодію всіх учасників мережі без посередників та надасть можливість працювати з різними вендорами, що в свою чергу, дозволить зменшити ціну на енергоресурси.

При розробці прототипу було використано мову програмування Java. При створенні системи були використані технології React.js, Node.js, MongoDB.

1. ЗАДАЧА РОЗРОБКИ АВТОМАТИЗОВАНОЇ СИСТЕМИ З ОБЛІКУ ЕНЕРГОРЕСУРСІВ НА ОСНОВІ БЛОКЧЕЙНУ

Система має проводити облік та торгівлю енергоресурсів, з використанням блокчейн технології.

На систему, що проектується, накладаються наступні вимоги:

— Система повинна бути децентралізована, кожен користувач повинен мати екземпляр програмного продукту;

— Користувач повинен керувати лише даними, які пов’язані з ним

— Користувач може переглядати будь-які дані, які знаходяться в блокчейні

— Користувач може вносити корисну інформацію (в даному випадку це дані про споживання енергоресурсів) і проводити оплату за енергоресурси за допомогою криптовалюти.

Крім того, система повинна мати зручний та сучасний графічний інтерфейс користувача з можливістю працювати у веб-браузері та бути імплементована відповідно до шаблонів задля гнучкого внесення змін та додавання нового функціоналу.

2. РОЗГЛЯД ТА АНАЛІЗ КОНЦЕПЦІЇ БЛОКЧЕЙНУ З ЕКОНОМІЧНОЇ ТА ТЕХНІЧНОЇ ТОЧКИ ЗОРУ

Концепція блокчейну була придумана Сатосі Накамото в 2008 року у вигляді системи «Біткоїн» яка дозволяла впровадити криптовалюту та проводити фінансові операції без посередників.

Наступні підрозділи описують можливості подальшого впровадження блокчейн технологій, зокрема в енергетичному секторі, та фундаментальний принцип, який застосовується в даній технології — хешування.

2.1 Розгляд блокчейн технологій та перспектива їх впровадження

Розвиток ІТ-технологій щодня пропонує світові нові інструменти для оптимізації бізнес-процесів. Одним з останніх таких інструментів є технологія ─ блокчейн (blockchain technology).

Думки експертів щодо ідеї впровадження криптовалют розділилися: одні вважають це справді революційним, але не зовсім зрозуміло, чи вдасться здійснити цю революцію. Другі ─ це інновації, які потребують значної адаптації та не є революційними. Тому питання подолання певної багатозначності їх віртуального і практичного використання е актуальними, та потребують подальшого дослідження.

В сучасних умовах прийнята технологія обліку і контролю енергоресурсів застаріла через організаційну та технічну недосконалість структур, що здійснюють облік. Ці проблеми стають причиною постійних збитків, що явно свідчить про необхідність створення сучасної автоматизованої системи.

Метою дослідження є аналіз перспектив та варіантів використання блокчейн технологій в енергетиці та розгляд алгоритму системи обліку споживання та платежів за енергоресурси.

Блокчейн ― технологія здатна докорінно змінити енергетичну систему, спочатку шляхом трансформації окремих секторів і, нарешті, шляхом трансформації всього ринку електроенергії.

Міжнародні енергетичні компанії розробляють проекти, які надалі з'єднають усіх споживачів в одну мережу ― децентралізовану систему. За допомогою розумних контрактів буде спрощена існуюча багаторівнева система, що складається з виробників електроенергії, операторів розподільної мережі, операторів-постачальників, постачальників платіжних послуг банківських послуг, споживачів та трейдерів. Усі транзакції щодо отримання та оплати за енергію здійснюватимуться безпосередньо в мережі, об'єднуючи рівних учасників ―споживачів та виробників енергії. Завдяки цьому електроенергія буде дешевою.

Крім того, всі транзакції будуть відкритими. Люди не зможуть прострочити платіж за споживання енергії ― розумний контракт контролюватиме виконання всіх операцій. Система сама заплатить за себе, тобто спише стільки криптовалюти, скільки Вам знадобиться для транзакції по передачі енергії.

Моделі транзакцій на блокчейні базуються на тому, що вся електроенергія, що подається в електромережу, може бути чітко віднесена до обліку конкретних споживачів за короткий проміжок часу. Це означає, що розрахунок за всю вироблену та спожиту електроенергію може бути дуже точно проведений за змінними цінами. Електрика буде продовжувати надходити до кінцевого споживача безпосередньо від найближчого виробника електроенергії. База даних, що зазнала значного поліпшення, дозволить точно «налаштувати» операції в мережі як на рівні передачі електроенергії, так і на рівні розподілу. Спрощений процес взаєморозрахунків призведе до зниження обсягу балансу енергії, на рахунки які виставляються учасникам ринку.

Завдяки блокчейну всі потоки електроенергії захищені від сторонніх маніпуляцій. Це дозволить сертифікувати електроенергію, перевірити квоти на допустимі викиди, кількість яких регулюється законодавством. Децентралізована технологія функціонує як база даних транзакцій, побудована за принципом розподіленого реєстру, тому за допомогою блокчейна можна створити універсальний

архів для зберігання всіх даних за виставленими рахунками за електроенергію. Споживачі отримають можливість розширеного контролю за своїми договорами на постачання електроенергії, а також дані про споживання електроенергії. Усі записи зберігатимуться у відкритому доступі в блокчейн-реєстрі, який буде коригувати всі питання права власності та поточний стан активів ─ розумних інтернет-речей (Інтернет речей, IoT) [1].

Технологія блокування, крім того, що використовується для проведення операцій з постачання енергії, може слугувати основою для процесів вимірювання кількості споживаної електроенергії, виставлення рахунків за споживання кількості та проведення розрахунків. Інші можливі додатки включають право власності на активи, управління активами, систему сертифікатів ─ "гарантоване походження", квоти на викиди вуглекислого газу та сертифікати, що підтверджують виробництво електроенергії на основі використання відновлюваних джерел енергії (ВДЕ). Можливості використання технологій в енергетиці представлені нижче

Таблиця 1 — Варіанти використання блокчейну в енергетиці

Транзакції і «розумні контракти»	**Права власності на активи і управління ними**	**Децентралізовані інформаційні системи**
Децентралізована торгівля електроенергією	Реєстрація власності та ведення реєстру активів	Облік електроспоживання та виставлення рахунків за електроенергію
Особливі можливості для просьюмерів	«Зелені» сертифікати	Облік споживання тепла і виставлення рахунків за нього
Впровадження криптовалют	Квоти на викиди вуглекислого газу і сертифікація виробництва електроенергії на основі відновлюваних джерел енергії	Оплата зарядки електромобілів
Зарядка електромобілів		
Управління розумними пристроями в інтернеті речей		

При об’єднані окремих блокчейн ─ додатків в майбутньому може з’явитися децентралізована система енергетичних транзакцій та постачання енергії. Постачання електроенергії, виробленої на об'єктах малої енергетики, кінцевими споживачами, здійснюватиметься через мікромережі. Кількість виробленої та спожитої електроенергії вимірюватиметься за допомогою розумних лічильників, а операції з торгівлі енергією та сплата криптовалютою контролюватимуться за допомогою смарт-контрактів та здійснюватимуться з використанням блокчейн.

Слід зазначити, що існуючі блокчейн ─ додатки можна розділити на три великі категорії залежно від рівня розробки, а саме: блокчейн-додатки версій 1.0, 2.0 та 3.0. Технологія блокчейн нового покоління, блокчейн 3.0, ще розробляється. Blockchain 3.0 ─ це етап розвитку технологій, на якому здійснюється подальший розвиток концепції "розумного контракту" з метою створення децентралізованих, автономних організаційних підрозділів, які керуються власними законами та працюють майже незалежно. Децентралізована система енергетичних транзакцій та постачання енергії представлена на (рис. 1.1).

Прозоре та децентралізоване врегулювання угод на вітчизняному енергетичному ринку збільшить частку електроенергії, отриманої від відновлюваних джерел енергії.

Блокчейн чітко фіксує джерело походження кожної кіловат-години в загальній мережі і дає покупцю гарантію, що він отримає енергію вітру, а не згенеровану газовою станцією.

Враховуючи все вище написане все, можна визначити такі перспективи і, одночасно, виклики у взаємозв'язку технологій блокчейн в Україні:

— шлях впровадження блокчейну в енергетику буде досить тривалим;

— відсутність стандартів, працюючих платформ, масштабних розподілених узгоджених системних і механізмів взаємодії - наявні технології на цьому етапі є дуже ризикованими;

Рисунок 1.1 — Децентралізована система енергетичних транзакцій і енергопостачання

— немає готових сильних рішень. На сьогоднішній день багато пілотних проектів і цікавих стартапів, але немає готових програмні продукти, які можна було почати використовувати в реальних бізнес-процесах;

— державна влада довго виставляє ініціатора та замовлення при внесенні технологій, що розширюють реестр та підтримують зворотну зв'язок із громадянами, беруть участь у «розумних» контрактах (Smart Contracts).

2.2 Опис алгоритму хешування

Вирішальне значення у концепції роботи блокчейну відіграє хешування. Саме завдяки хешуванню можливо проводити майнинг та будувати зв’язані блоки. Нижче буде наведено опис роботи алгоритму SHA-1.

Алгоритми хешування перетворюють текст будь-якої довжини у текст з фіксованою довжиною. Дані алгоритми забезпечують логічну цілісність тексту, валідність паролів та широко використовуються у криптографічних системах [7].

Важливі 2 особливості хешування:

— один і той же текст в різні моменти часу буде генерувати алгоритмом одне і те ж хеш-значення;

— алгоритми односторонні — хеш-значення неможливо перетворити у звичайний текст.

Хід роботи алгоритму представлений нижче:

Ініціалізація змінних у двійковому форматі:

Ділення тексту на слова.

Ділення тексту на букви.

Переведення букв в ASCII код.

Переведення ASCII коду в бінарний вигляд:

Об’єднання бінарного коду:

Додавання бітової «1» в кінець бінарного коду:

Додавання бітових «0» в бінарного коду допоки довжина бінарного коду не буде складатися 449 бітів:

Додавання в кінець бінарного коду довжини оригінального тексту з попереднім додаванням нулів допоки довжина бінарного коду не буде 512 бітів

Розділення бінарного коду на 16 32-бітні слова та присвоєння змінній chunk.

Далі необхідно на основі отриманих 16 слів вивести ще 64 32-бітні слова.

Оголошується локальна змінна в інтервалі [16, 79] і запускається цикл з її інкрементуванням:

Подальший процес повторюється на кожній ітерації:

4 слова присвоюється змінним wordA, wordB, wordC, wordD:

$$\begin{cases} wordA = chunk[i-3] \\ wordB = chunk[i-8] \\ wordC = chunk[i-14] \\ wordD = chunk[i-16] \end{cases}$$

Проводиться операція взаємовиключаючого «АБО» (XoR) у наступному

порядку з присвоєнням змінних:

$$\begin{cases} xorA = wordA \oplus wordB \\ xorB = xorA \oplus wordC \\ xorC = xorB \oplus wordD \end{cases}$$

У змінній xorC проводимо процес зміщення бітів вліво на 1 і додається результат у 32 бітний код.

Після завершення ітерації отримується бітовий код, що складається з 80 слів:

Ініціюються змінні:

A = h0
B = h1
C = h2
D = h3
E = h4

Запускається цикл по масиву бітових значень, виведеному раніше. По кожному бітовому значенню запускається внутрішній цикл із інкрементуванням локальної змінної в інтервалі [0, 79] з виконанням операцій:

$$\begin{cases} \boldsymbol{f1}, & \boldsymbol{i \geq 0\ AND\ i \leq\ 19} \\ \boldsymbol{f2}, & \boldsymbol{i \geq 20\ AND\ i \leq\ 39} \\ \boldsymbol{f3}, & \boldsymbol{i \geq 40\ AND\ i \leq\ 59} \\ \boldsymbol{f4}, & \boldsymbol{i \geq 60\ AND\ i \leq\ 79} \end{cases}$$

Далі опишемо роботу функцій f1, f2, f3, f4. В них виконуються побітові операції і присвоюється значення змінній K.

$$\boldsymbol{f1 = (B \wedge C) \vee (!\,B \wedge D)}$$

$$\boldsymbol{f2 = B \oplus C \oplus D}$$

$$\boldsymbol{f3 = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)}$$

$$\boldsymbol{f4 = B \oplus C \oplus D}$$

Далі в рамках того ж циклу в змінній temp зберігається результат обчисленняя:

$$temp = (A\ left\ rotate\ 5) + F + E + K + (word)$$

де word – бітове слово отримуване на кожній ітерації циклу.

Обрізається змінна temp до розміру в 32 біти і виконується останній набір обчислювальних операцій під час кожної ітерації:

E = D
D = C
C = B Left Rotate 30
B = A
A = temp

Отримані бітові значення переводяться в шістнадцятковий формат і об’єднуються в єдиний текст:

8f0c0855915633e4a7de19468b3874c8901df043

Окрім алгоритму SHA-1 існують модифіковані алгоритми хешування які унеможливлюють зламування хешу методом перебору за рахунок того, що наприклад SHA-2 на виході утворює хеш-значення довжиною 224 або 256 бітів, натомість як SHA-1 лише з довжиною 160 [7].

3 ЗАСОБИ РОЗРОБКИ

При створенні системи важливе значення мають обрані технології реалізації. Для проектування системи була обрана мова програмування Java, яка має велику кількість стандартних бібліотек з інкапсульованим функціоналом.

При проектуванні повноцінної автоматизованої системи було обрано мову Javascript з використанням фреймворків Node.js, React.js, а для збереження інформації була обрана база даних MongoDB.

Припускається, що система буде працювати в мережі Інтернет. Вся взаємодія між користувачем та системою в мережі Інтернет відбувається за допомогою протоколу HTTPS. Передача даних здійснюється на основі архітектурного шаблону REST, де всі операції маніпулювання з даними в рамках Інтернету виконуються за допомогою 4 типів HTTP запитів:

— GET – на отримання інформації;
— POST – на збереження інформації;
— PUT – на оновлення інформації;
— DELETE - на видалення інформації.

Корисна інформація в рамках HTTP запитів передається у форматі JSON.

Реалізована система використовує перші два типи запитів.

3.1 MongoDB

MongoDB реалізує новий підхід до побудови баз даних, де немає таблиць, схем, запитів SQL, зовнішніх ключів і багатьох інших речей, які притаманні реляційним базам даних.

На відміну від реляційних баз даних MongoDB пропонує документо-орієнтовану модель даних, завдяки чому MongoDB працює швидше, має кращу

масштабованість, її легше використовувати.

Але, навіть враховуючи всі недоліки традиційних баз даних і переваг MongoDB, важливо розуміти, що завдання бувають різні і методи їх вирішення бувають різні. В якійсь ситуації MongoDB дійсно підійде для реалізації, наприклад, якщо треба зберігати складні за структурою дані. В іншій же ситуації краще буде використовувати традиційні реляційні бази даних. Крім того, можна використовувати змішані підходи: зберігати один тип даних в MongoDB, а інший тип даних - в традиційних БД.

Вся система MongoDB може бути представлена різними вузлами на різних фізичних машинах і ці бази даних зможуть легко обмінюватися даними і зберігати цілісність.

Одним з популярних стандартів обміну даними та їх зберігання є JSON (JavaScript Object Notation). JSON ефективно описує складні за структурою дані. Спосіб зберігання даних в MongoDB в цьому плані схожий на JSON, хоча формально JSON не використовується. Для зберігання в MongoDB застосовується формат, який називається BSON або скорочення від «Binary JSON».

BSON дозволяє працювати з даними швидше: швидше виконується пошук і обробка. Хоча треба зазначити, що BSON на відміну від зберігання даних в форматі JSON має невеликий недолік: в цілому дані в JSON-форматі займають менше місця, ніж в форматі BSON, з іншого боку, даний недолік окупається швидкістю.

MongoDB написана на C++, тому її легко перенести на найрізноманітніші платформи. MongoDB може бути розгорнутий на платформах Windows, Linux, MacOS, Solaris. Можна також завантажити код і самому скомпілювати MongoDB, але рекомендується використовувати офіційні бібліотеки.

Якщо реляційні бази даних зберігають кортежі, то MongoDB зберігає документи. На відміну від термін документи можуть зберігати складну за структурою інформацію. Документ можна представить як сховище ключів і значень.

Ключ являє просту мітку з яким асоційовано певний набір даних.

Однак при всіх відмінностях є одна особливість, яка зближує MongoDB і реляційні бази даних. У реляційних СУБД зустрічається таке поняття як первинний

ключ. Це поняття описує якийсь стовпець з автоматично створеним індексом який ідентифікує унікальний запис. У MongoDB для кожного документа є унікальний ідентифікатор, Який називається “_id”. І якщо явно не указ його значення, то MongoDB автоматично згенерує для нього значення.

Кожному ключу зіставляється певне значення. Але тут також треба враховувати одну особливість: якщо в реляційних базах є чітко окреслена структура, де є поля, і якщо якесь поле не має значення, йому (в залежності від налаштувань конкретної бд) можна привласнити значення NULL. У MongoDB все інакше. Якщо ключ не має значення, то він просто опускається в документі і не вживається.

Якщо в традиційно світі SQL є таблиці, то в світі MongoDB є колекції. І якщо в реляційних БД таблиці зберігають однотипні жорстко структуровані об'єкти, то в колекції можуть містити найрізноманітніші об'єкти, що мають різну структуру і різний набір властивостей.

Система зберігання даних в MongoDB представляє набір реплік. У цьому наборі є основний вузол, а також може бути набір вторинних вузлів. Всі вторинні вузли зберігають цілісність і автоматично оновлюються разом з оновленням головного вузла. І якщо основний вузол з якихось причин виходить з ладу, то один з вторинних вузлів стає головним.

Відсутність жорсткої схеми бази даних і в зв'язку з цим потреби при щонайменшій зміні концепції зберігання даних створювати нову схему значно полегшують роботу з базами даних MongoDB і подальшим їх масштабуванням. Крім того, економиться час розробників. Їм більше не треба думати про створення нової схеми бази даних і витрачати час на побудову складних запитів.

3.2 Опис мови програмування Java

Для створення прототипу системи була обрана мова програмування Java з наступних причин:

ООП: в Java все є об'єктом. Клас може бути легко розширено, тому що він

заснований на об'єктної моделі.

Платформонезалежність: на відміну від багатьох інших мов, включаючи C і C++, Java, коли була створена, вона не компілювалася в платформі конкретної машини, а в незалежному від платформи байт-коді. Цей байт інтерпретується в Java Virtual Machine (JVM), на якій він в даний час працює.

Простота: процеси вивчення та введення в мову програмування Java залишаються простими.

Архітектурна нейтральність: компілятор генерує архітектурно-нейтральні об'єкти формату файлу, що робить скомпільований код виконуваним на багатьох процесорах

Міцність: докладаються зусилля, щоб усунути помилки в різних ситуаціях, спираючись в основному на час компіляції, перевірку помилок і перевірку під час виконання.

Багатопоточність: функції багатопоточності, можна писати програми, які можуть виконувати безліч завдань одночасно. Введення в мову Java цієї конструктивної особливості дозволяє розробникам створювати налагоджені інтерактивні додатки.

Інтерпретованість: Java байт-код переводиться під виконання в машинні інструкції та ніде не зберігається. Роблячи процес більш швидким і аналітичним, оскільки зв'язування відбувається як додаткове з невеликою вагою процесу.

Високопродуктивність: введення Just-In-Time компілятора, дозволило отримати високу продуктивність.

Динамічність: програмування на Java вважається більш динамічним, ніж на C або C ++, так як призначення до адаптації в мінливих умовах.

4 ОПИС ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

Автоматизована система розроблена за принципом «Клієнт-сервер» і здатна працювати в мережі Інтернет. Кожен користувач повинен завантажити на локальну машину екземпляри серверів та завантажити репліку блокчейну.

4.1 Опис алгоритму роботи блокчейну в автоматизованій системі з обліку енергоресурсів

Блокчейн – це система, яка дозволяє організувати однорангову взаємодію в мережі без посередників і прямим доступом до інформації всім учасникам мережі [8]. Завдяки своїй структурі і принципу роботи, в системі неможлива підробка даних (тому що для підробки необхідно буде використовувати колосальні обчислювальні ресурси, які в кінцевому результаті не зможуть окупитися).

Принцип роботи полягає в тому, що існує ланцюжок (chain). Ланцюжок складається з блоків. Транзакції, які, в свою чергу, формують користувачі системи (наприклад на переказ грошей) формуються в блоки. Кожен блок, крім набору транзакцій, які в нього записані, містить хеш значення, засноване на даних, які містяться в цьому блоці (в тому числі і транзакції), що обчислюється алгоритмом SHA-2. Всі блоки шукуються в чергу в порядку їх створення. Поточний блок окрім обчисленого хеш значення на основі власних даних, містить хеш-значення попереднього блоку. Хеш значення попереднього блоку також бере участь в обчисленні хеш-значення поточного блоку. Саме ця особливість і формує ланцюжки. Зміна хоч одного символу призведе до кардинальної зміни хеш-значення, що призведе, у свою чергу, до зміни хеш-значення всіх наступних блоків (це буде говорити про те, чи була здійснена спроба підробити дані) [8].

Транзакції повинні містити адресу відправника, адресу реципієнта, час

створення транзакції, корисну інформацію, цифровий підпис. Адреси відправника та реципієнта є гаманцями користувачів. Адреси реалізовані за допомогою асиметричного шифрування і представлені у вигляді публічного ключа, який доступний всім користувачів мережі. Час створення транзакції представлено у вигляді часової мітки (timestamp). Для успішної роботи в мережі блокчейну, користувач повинен мати пару згенеровану із публічного та приватного ключа. Приватним ключем, який доступний тільки власнику цього ключа можливо створити цифровий підпис, який буде задовольняти позитивного результату при порівнянні підписи і публічного ключа. Цей процес дозволяє підтвердити, що не було підроблено публічний ключ.

Рисунки наведені нижче демонструють принцип роботи блокчейну у вигляді блок-схем.

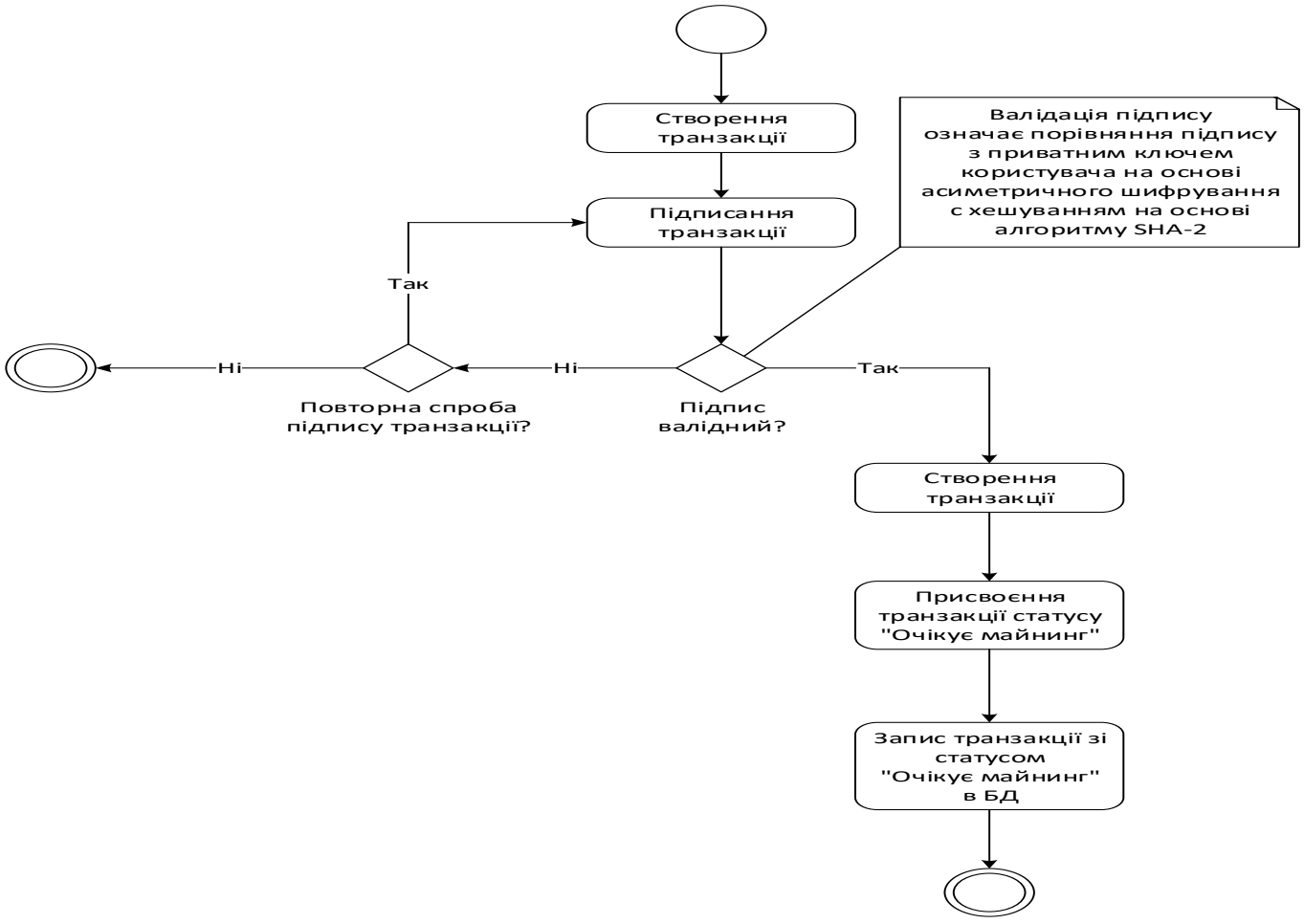


Рисунок 2.1 — Алгоритм створення транзакції

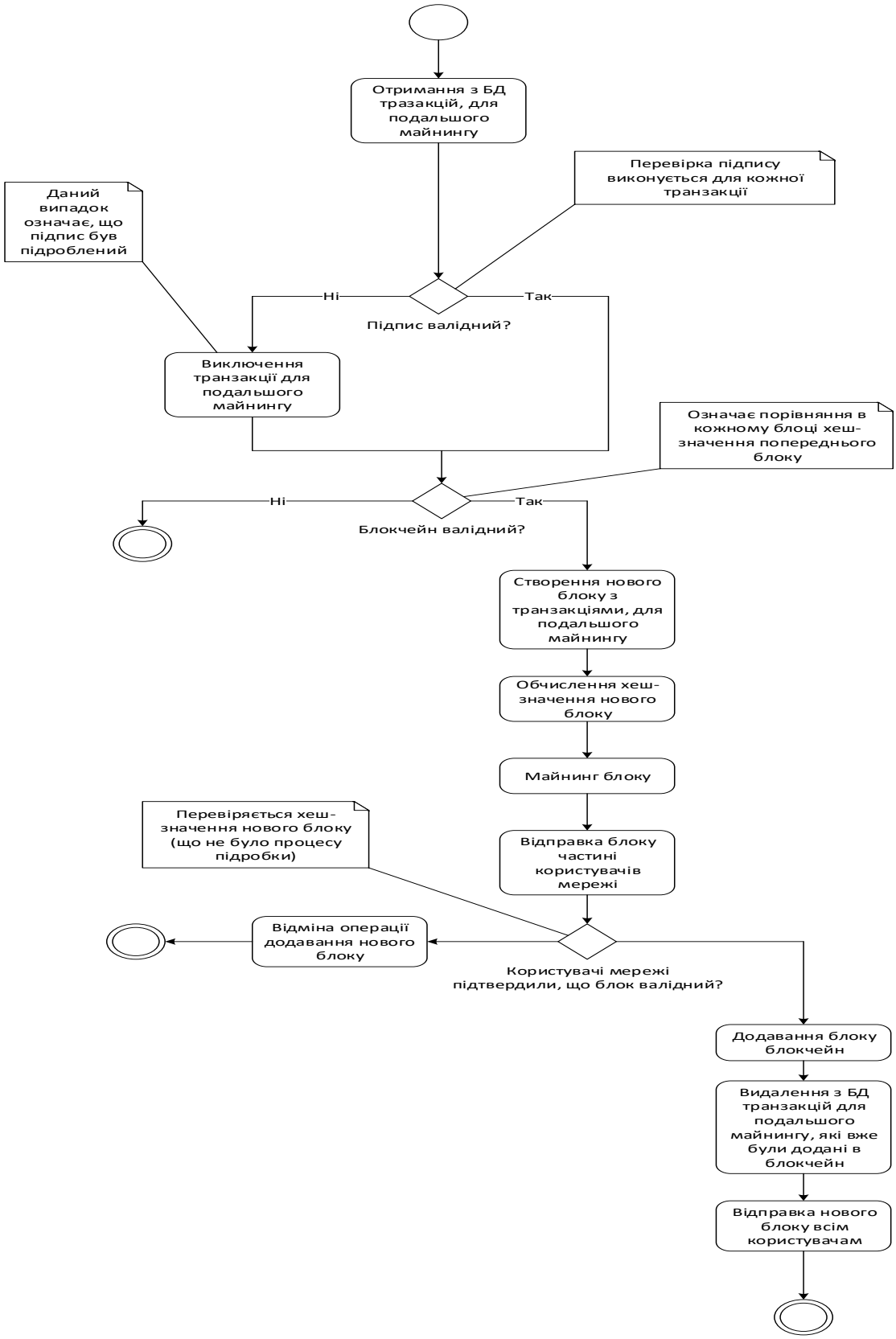


Рисунок 2.2 — Алгоритм оновлення блокчейну від початку вибору транзакцій до внесення нового блоку у ланцюжок

Ще одним важливим аспектом в блокчейні є процес доказу роботи (proof-of-work), або по-іншому ще названий майнингом. Хеш значення всіх блоків зміщені на певну кількість нулів. Кількість нулів визначено змінною, яка називається складністю (difficulty). У процесі обчислення хеш-значення бере участь ще одна змінна, яка називається поточним значенням (nonce). В процесі майнингу, змінна nonce інкрементується, що призводить до рекалькуляції хеш-значення. Рекалькуляція буде відбувається до того моменту, поки всі символи хеш-значення в інтервалі [0, difficulty] не будуть складатися з нулів. Час роботи майнингу збільшується експоненціально від складності, що дозволяє регулювати тривалість цього процесу в залежності від об'єму обчислювальних потужностей в мережі.

Після того, як було проведено успішний майнинг блоку, він відправляється всім, або більшої частини учасників мережі, кожен з яких перевіряє ланцюжок на валідність з урахуванням нового блоку. Суть перевірки полягає в тому, що в кожному блоці рекалькулюється хеш-значення. Так як блок зберігає хеш-значення самого себе і хеш-значення попереднього блоку, відбувається перевірка по кожному блоку: в поточному блоці порівнюється збережене хеш-значення попереднього блоку з хеш-значенням попереднього блоку. Якщо більша частина (або всі) учасники мережі підтвердять, що перевірка успішна, блок додається в ланцюг, всі учасники мережі оновлюють ланцюжок з новим блоком.

4.2 Опис архітектури

Система по своїй суті представлена у вигляді децентралізованої мережі вузлів для кожного користувача з однаковим функціоналом в залежності від ролі (користувач системи, майнер) та одного завантажуючого сервера (bootstrapper server) який виконує інфраструктурну задачу ─ проводить синхронізацію користувачів між собою. Завантажуючий сервер містить колекцію (в термінах mongoDB) користувачів (пул користувачів).

Для того, щоб почати роботу із системою, користувачеві необхідно запустити у себе на локальній машині сервер, який приймає запити і виконує обробку даних (back-end server); та сервер, який надає графічний інтерфейс користувача (front-end server).

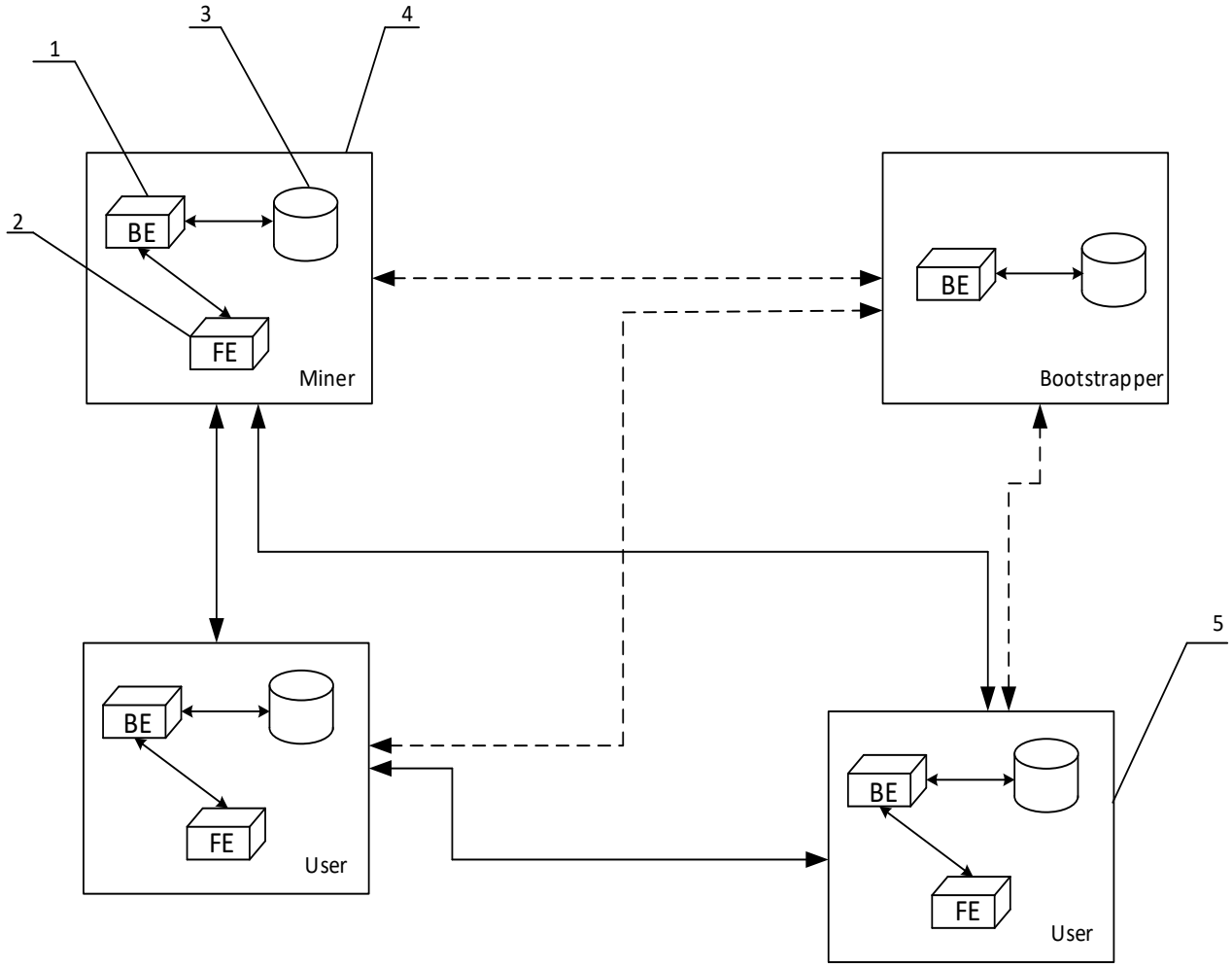
У мережі наявно 2 ролі користувачів: користувач, що виконує майнинг блоків; користувач, що виконує створення транзакцій. Кожен екземпляр пари серверів обробки даних та графічного інтерфейсу користувача являє собою вузол мережі.

Під час проектування архітектури було прийнято рішення впровадити даний сервер для розділення обов'язків. Сервер повинен виконувати одну і лише одну задачу. Бо у випадку внесення змін у програмний код, або додавання нового функціоналу, код може стати сильно зав'язаним один із одним (у випадку відсутності розділення функціоналу), і його стане важко супроводжувати в подальшому. Також було прийнято рішення, що у випадку, коли блокчейн не має ні одного блоку, а мережа ні одного користувача, завантажуючий сервер створює перший блок (genesis block).

Між користувачем та завантажуючим сервером здійснюється взаємодія для отримання даних про інших користувачів мережі. Аналогічний принцип роботи між майнером та завантажуючим сервером.

Робота між майнером та користувачем полягає у тому, що майнер отримує транзакції від користувача і після здійснення майнингу блоку здійснює поширення (broadcasting) всім вузлам нового блоку; якщо блок пройшов валідацію і не був раніше доданий до блокчейну — він додається, майнер отримує грошову винагороду за пророблену роботу.

Концепція роботи між користувачем та майнером полягає у тому, що користувач створює транзакцію і поширює її всім майнерам. Рисунки 4.1 — 4.3 демонструють приклади мережі, діаграму прецедентів та діаграму класів автоматизованої системи.



Умовні позначення:

1 – оброблюючий сервер (back-end server)

2 – сервер графічного інтерфейсу користувача

3 – локальна база даних користувача

4, 5 – вузол блокчейн мережі

⟷ - двонаправлений зв’язок для обміну даними в межах вузла

⟷ - двонаправлений зв’язок для обміну даними між вузлами в мережі

⟷ - двонаправлений зв’язок для обміну даними між вузлом мережі та запускаючим сервером

Рисунок 4.1 — Приклад мережі з двома користувачами та одним майнером

Рисунок 4.2 — Діаграма прецедентів системи, що проектується

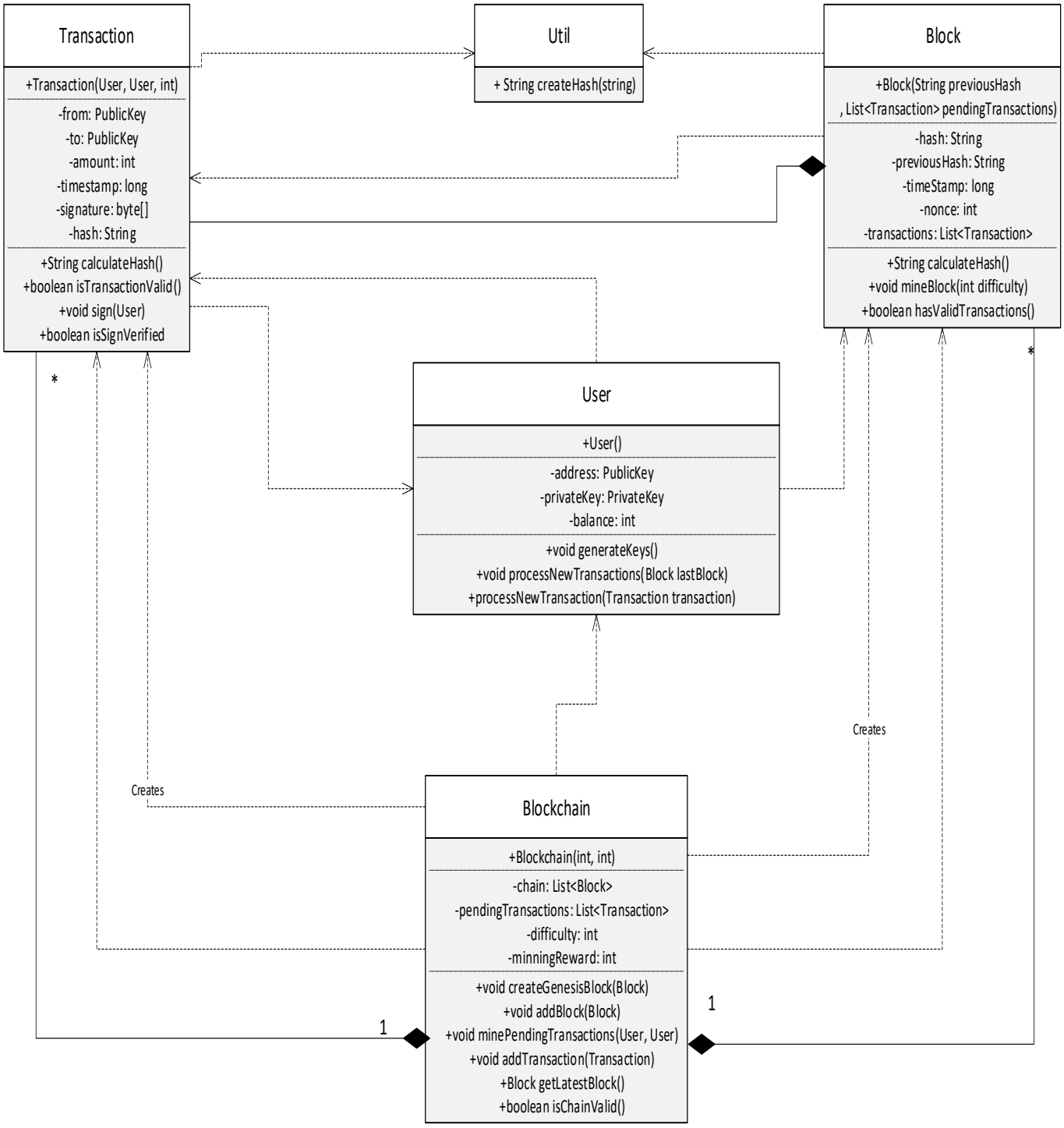


Рисунок 4.3 — Діаграма класів системи, що проектується

Блокчейн можливо описати у вигляді сутностей, які зберігають інформацію і формують ядро всієї системи (таблиці 4.1 – 4.2)

Таблиця 4.1 – сутність «Блок»

Назва поля	**Тип даних**	**Опис і призначення**
hash	Текстове значення	Буквенно-чисельне значення форматоване в текст і обчислене за допомогою алгоритмів хешування. Унікальний ідентифікатор блоку
previousHash	Текстове значення	Буквенно-чисельне значення форматоване в текст і обчислене за допомогою алгоритмів хешування. Унікальний ідентифікатор поперенього блоку
date	Текстове значення	Дата створення блоку
nonce	Чисельне значення	Число, при якому метод доказу зупинився обчислювати хеш-значення (а отже було доведено що блок не підроблений)
transactions	Масив сутностей	Список транзакцій
minerReward	Чисельне значення	Нагорода у вигяді криптовалюти, яка надається майнеру після закінчення процесу доказу роботи

Таблиця 4.2 – сутність «Транзакції»

Назва поля	**Тип даних**	**Опис і призначення**
from	Текстове значення	Буквенно-чисельне значення, форматоване в текст і обчислене за допомогою криптографічних алгоритмів. Адреса електронного гаманця користувача, який бажає переказати криптовалюту. Являється публічним ключем користувача
to	Текстове значення	Буквенно-чисельне значення, форматоване в текст і обчислене за допомогою криптографічних алгоритмів. Адреса електронного гаманця користувача, який буде отримувати криптовалюту . Являється публічним ключем користувача
amount	Чисельне значення	Сумма переказу криптовалюти
signature	Текстове значення	Буквенно-чисельне значення, форматоване в текст і обчислене за допомогою криптографічних алгоритмів. Формується приватним ключем користувача
description	Текстове значення	Опис транзакції. Вводиться користувачем.

Засоби мови Javascript надають інкапсульований функціонал з генерації приватних та публічних ключів, хешування інформації, що використовуються в проекті.

4.3 Механізм авторизації та аутентифікації користувачів за допомогою JSON Web tokens

Процес генерації токена:

Здійснюється сервером на основі запитів POST /signup, POST /login. При подальших запитах якщо сервер не знайде токену, то видасть у відповіді помилку 401 з описом проблеми.

Перевірка токена:

Здійснюється перевірка заголовку Autorization на наявність тексту. Якщо він відсутній – відправляється повідомлення "No token provided". Якщо текст присутній – здійснюється валідація токена і пошук користувача; якщо процес успішний – HTTP запит виконується, в іншому випадку – забороняється.

4.4 Алгоритм валідації нового блоку

Для визнання блоку валідним, необхідно виконання наступних умов:

— Попереднє хеш-значення в новому блоці повинно співпадати з хеш-значенням попереднього блоку.

— Хеш-значення що вказане в новому блоці повинно співпадати, якщо його перерахувати хеш-значенням за полями:

```
- previous hash (хеш-значення попереднього блоку)
- transactions (массив транзакцій блоку)
- nonce (число, яке було отримано під час майнингу блоку)
- date (дата створення блоку)
```

При умові виконання цих двох умов новий блок вважається валідним, його ніхто не підробив і його можна заносити в блокчейн.

5 Робота користувача з програмною системою

Даний розділ демонструє процес створення транзакції та внесення нової інформації в блокчейн в графічному інтерфейсі користувача та в базі даних.

5.1 Системні вимоги для додаткове програмне забезпечення

Для роботи з блокчейном накладаються вимоги з продуктивності роботи апаратного забезпечення.

Для роботи мінімально необхідні: процессор Intel Core i3, 8 Гб оперативної пам'яті, 256 ГБ вільного місця на жорсткому диску.

Додатково необхідно встановити MongoDB, NPM для збережння блокчейну на локальній машині та для запуску серверів.

5.2 Результати виконання програми

Після того, як користувач зареєструвався та увійшов в систему, він має можливість переглянути дії, які здійснювали всі користувачі раніше у вигляді логу ініційованих транзакцій (вкладка «View blockchain»), де показано від кого транзакція відправляється, кому віправляється, сумма переказу, хеш-значення електронних гаманців користувачів (рисунок 5.1).

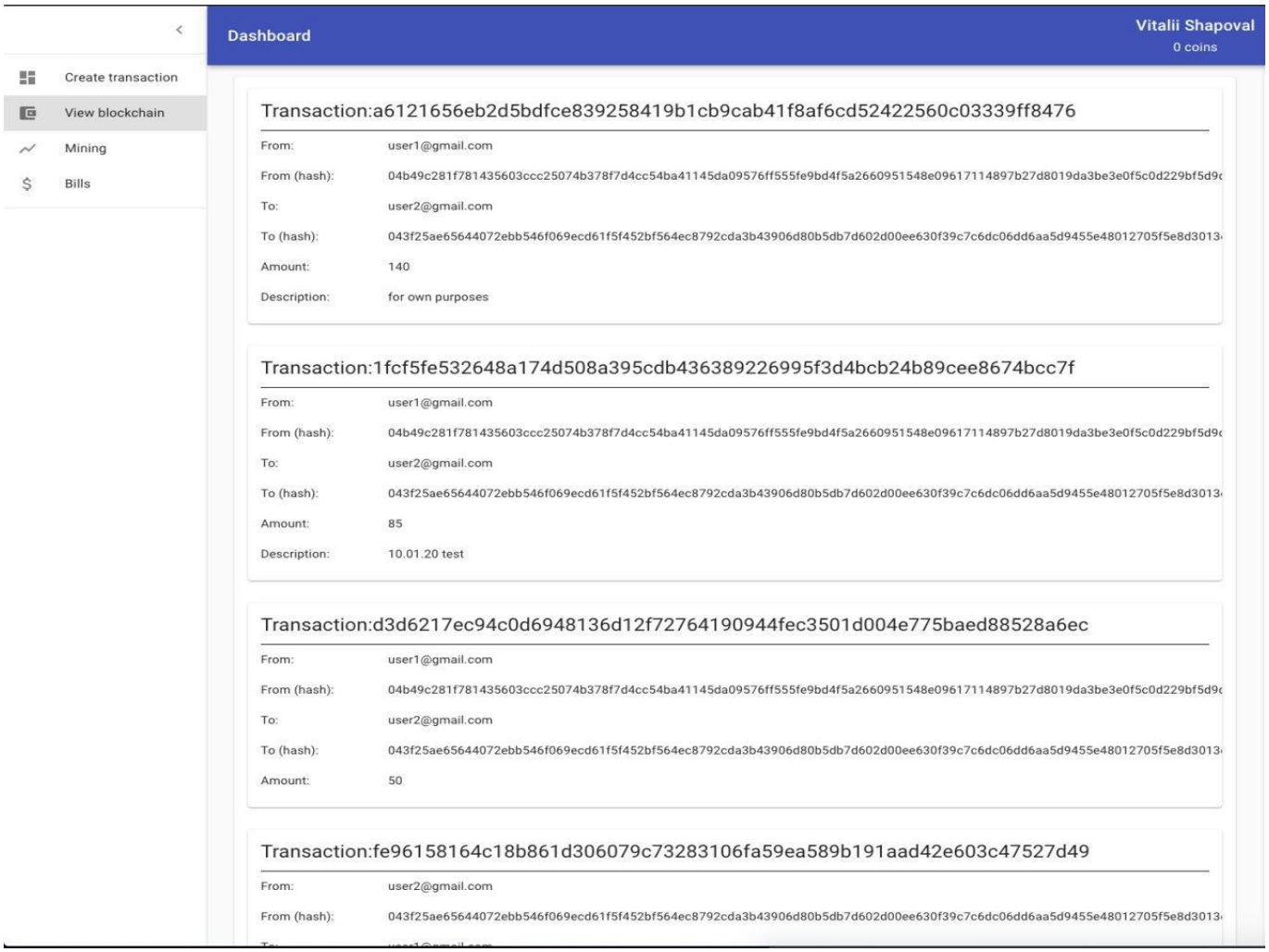


Рисунок 5.1 — Сторінка списку транзакцій

До моменту створення нової транзакції і її майнингу, таблиця, яка їх зберігає, представлена на рисунку 5.2.

Рисунок 5.2 — Останній блок (виділено червоним) до майнингу нового блоку, представленого в графічному інтерфейсі

У випадку, якщо користувач хоче ініціювати новий переказ, йому необхідно перейти на вкладку «Create transaction» (рисунок 5.3), вказати хеш-значення електронного гаманця, суму переказу та короткий опис транзакції, якщо це необхідно.

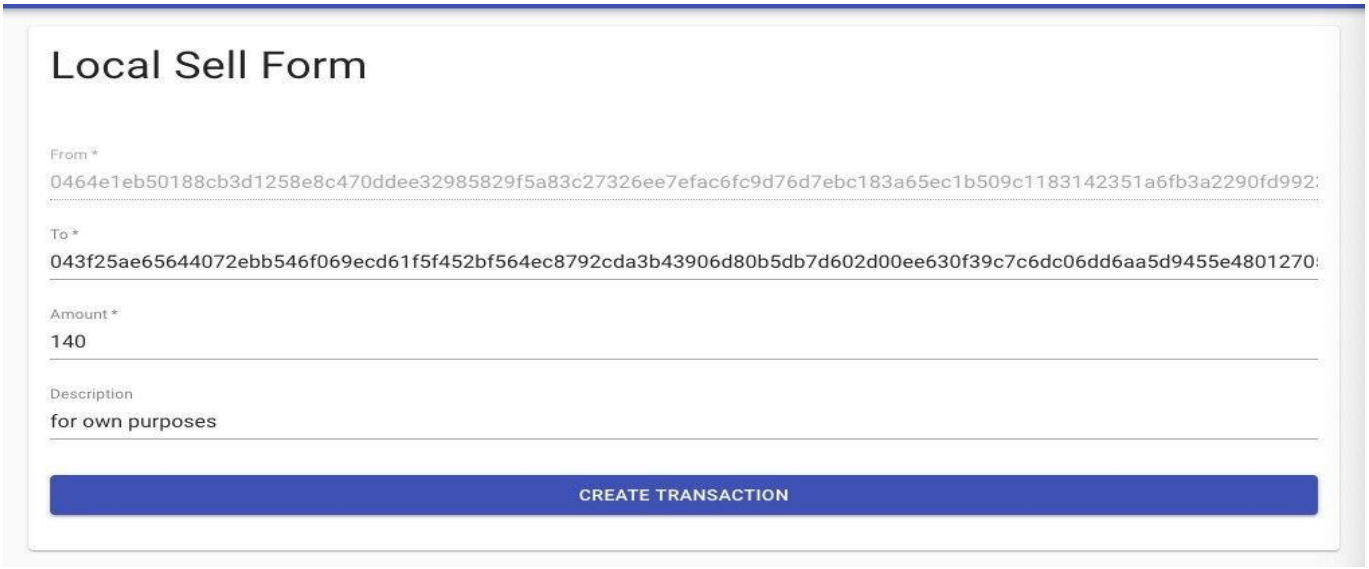


Рисунок 5.3 — Сторінка створення транзакції

Після того, як користувач ініціював транзакцію, вона потрапляє в пул транзакцій, які очікують майнингу.

База даних до моменту майнингу нового блоку представлена на рисунку 5.4. Коллекція зберігає всі блоки, які включають в собі хеш-значення блоку, хеш-значення попереднього блоку, дату створення блоку, значення (змінна «nonce») при якому майнинг блоку був завершений, набір транзакцій.

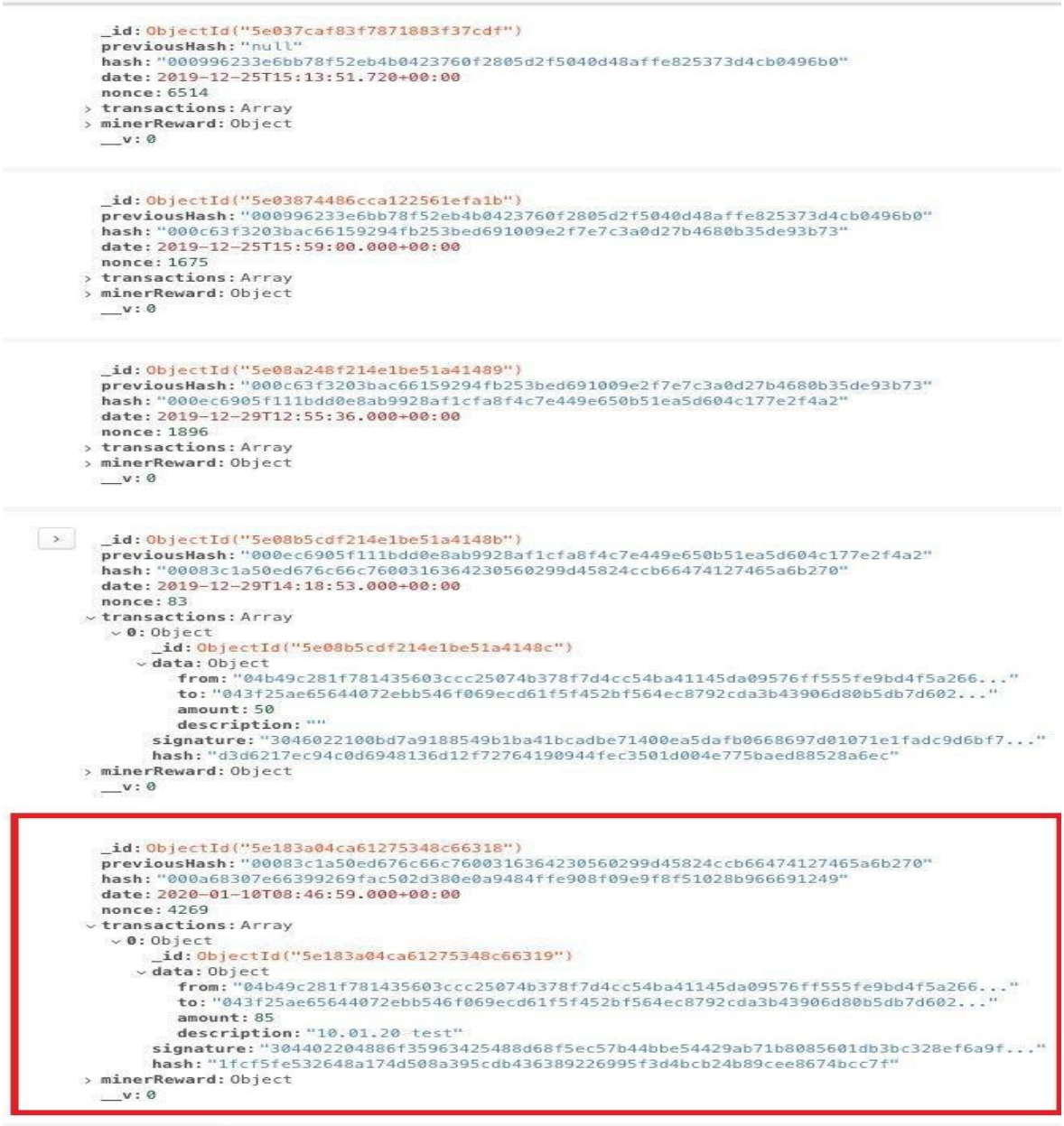


Рисунок 5.4 — Останній блок (виділено червоним) до майнингу нового блоку, представленого в базі даних

Після успішного майнингу нового блоку, транзакція з’явиться у вікні «View blockchain» (рисунок 5.5).

Рисунок 5.5 — Останній блок (виділено зеленим) та передостанній блок (виділено червоним) після майнингу нового блоку, представленого в графічному інтерфейсі

Репліка бази даних після майнингу нового блоку представлена на рисунку 5.6. Варто звернути увагу на поля «previousHash» найнижчого блоку та поле «hash» передостаннього блоку. Вони однакові. Саме даний принцип і дозволяє організовувати блокчейн

Рисунок 5.6 — Останній блок (виділено зеленим) та передостанній блок (виділено червоним) після майнингу нового блоку, представленого в базі даних

ВИСНОВКИ

В ході виконання даної роботи було проведено аналіз предметної області, включаючи аналіз вимог, вибір технологій, аналіз архітектури системи, організацію програмного коду. Було створено першу версію автоматизованої системи з ядром, виконаним на блокчейн технології яка дозволяє проводити облік та торгівлю енергоресурсів. Користувачами системи можуть бути особи, які зацікавлені у проведенні та обліку енергоресурсів. Спроектована автоматизована система має можливість проводити облік та продаж енергоресурсів різноманітних типів.

В системі закладено фундамент для подальшої розробки нового функціоналу: впровадження роботи зі смарт-контрактами; інтеграція із зовнішніми сервісами; автоматизовану систему генерування рахунків на основі показань лічильників; додавання бізнес-логіки, яка б дозволяла організовувати взаємодію користувачів як постачальників різноманітних енергоресурсів (як класичних, так і відновлювальних), так і звичайних споживачів, які могли би без посередників отримувати більш дешеві енергоресурси.

Практичне значення результатів полягає у забезпеченні приватності даних користувачів в технологіях на основі блокчейну, підвищення рівня децентралізації та удосконалення інших характеристик даної системи. Як наслідок, збільшиться коло застосування даної технології та знайдуться нові форми і сфери для її реалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сегеда І.В., Локотарев Є.О., Шаповал В.О. Реалізація використання блокчейн-технологій у енергетичному секторі. / Вчені записки Таврійського національного університету імені В.І. Вернадського Серія: Економіка і управління Том 30 (69). № 4, 2019, С. 160-165 (DOI: https://doi.org/10.32838/2523-4803/69-4-51) .
2. Segeda I. Blockchain as a digital economy promotion tool in energy industry. Modern Aspects of Software Development: Proceedings of VI International Scientific and Practical Virtual Conference of Software Development Specialists, June, 24 2019 p. – Kyiv: Igor Sikorsky KPI, 2019. – p. 139-146 .
3. Элина Редих. Что такое Blockchain и где его применяют в Украине [Електронний ресурс]. /– Режим доступу до ресурсу: https://biz.censor.net.ua/resonance/3061113/chto_takoe_blockchain_i_gde_ego_primenyayut_v_ukraine
4. Цифровая энергетика: видение, практики, технологии : Информационно-аналитические работы 2018 г. / Инфраструктурный Центр EnergyNet. — [б. м.] : [б. и.], 2018. — 224 с.
5. How Blockchain Technology Works. Guide for Beginners [Електронний ресурс] / – Режим доступу до ресурсу: https://cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners#distributed-database
6. Блокчейн: как он работает, и почему эта технология изменит мир [Електронний ресурс] /– Режим доступу до ресурсу: https://habr.com/ru/company/iticapital/blog/340992/
7. Hash Algorithms [Електронний ресурс] / – Режим доступу до ресурсу: https://www.metamorphosite.com/one-way-hash-encryption-sha1-data-software
8. Nakamoto S. A Peer-to-Peer Electronic Cash System [Електронний ресурс] // Bitcoin. – Режим доступ до ресурсу: https://bitcoin.org/bitcoin.pdf

9. SQL или NoSQL — вот в чём вопрос [Електронний ресурс] / – Режим доступу до ресурсу: https://habr.com/ru/company/ruvds/blog/324936/
10. NewSQL = NoSQL+ACID [Електронний ресурс] / – Режим доступу до ресурсу: https://habr.com/ru/company/odnoklassniki/blog/417593/
11. Гагарина Л. Г. Технология разработки программного обеспечения / Л. Г. Гагарина, Е. В. Кокорева, Б. Д. Виснадул. – Москва: ИД ФОРУМ, ИНФРА-М, 2008. – 400 с.
12. Соммервилл И. Инженерия программного обеспечения / Иан Соммервилл. – М.: Издательский дом Вильямс, 2002. – 624 с. – (6-е издание).
13. Боєм Б. У. Инженерное проектирование программного обеспечения / Б. У. Боєм. — М.: Радио и связь, 1985. — 512 с.
14. Мартин, Садаладж, Прамодкумар Дж. NoSQL: новая методология разработки нереляционных баз данных. : Пер. с англ. - М.: ООО "И.Д. Вильяме", 2013. - 192 с.: ил. - Парал. тит. англ.
15. Хорстманн К., Корнелл Г. Java 2. Библиотека профессионала. Т. 1, 2. — М.: Виль-ямс, 2010. — 816 с., 992 с.
16. Эккель Брюс. Философия Java. Библиотека программиста. — 4-е изд. — СПб.: Пи-тер, 2009. — 640 с.
17. Бадд Т. Объектно-ориентированное программирование в действии: Пер. с англ. — СПб.: Питер, 1997. — 464 с. Буч Г. Объектно-ориентированный анализ и проектирование с примерами приложений: Пер. с англ. — 3-е изд.—М.: Вильямс, 2010. — 720 с.
18. Коуд П., Норт Д., Мейфилд М. Объектные модели. Стратегии, шаблоны и приложения: Пер. с англ. — М.: Лори, 1999. — 446 с.
19. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж. Приемы объектно-ориентированного проектирования. Паттерны проектирования. — СПб.: Питер, 2005. — 368 с.
20. Стелтинг С., Маассен О. Применение шаблонов Java. Библиотека профессионала:Пер. с англ. — М.: Вильямс, 2002. — 576 с.

21. Bruce Eckel. Thinking in Patterns with Java. — 2004.[Електронний ресурс]. /– Режим доступу до ресурсу:http://mindview.net/Books/TIPatterns/
22. Ларман К. Применение UML 2.0 и шаблонов проектирования: Пер. с англ. — М.:Вильямс, 2009. — 736 с.
23. Вирт Н. Алгоритмы и структуры данных: Пер. с англ. — М.: Невский диалект,2008. — 352 с.
24. Ярмола Ю. А. Компьютерные шрифты. — СПб.: BHV — Санкт-Петербург, 1994. —208 с.
25. Блох Дж. Java. Эффективное программирование: Пер. с англ. — М.: Лори, 2008. —223 с.
26. Хабибуллин И. Ш. Создание распределенных приложений на Java 2. — СПб.: БХВ-Петербург, 2002. — 704 с.
27. Перри Б. У. Java сервлеты и JSP. Сборник рецептов. М.: КУДИЦ-Пресс, 2009. —768 с.
28. Хабибуллин И. Ш. Самоучитель XML. — СПб.: БХВ-Петербург, 2003. — 336 с.
29. Мак-Лахлин Б. Java и XML: Пер. с англ. — СПб.: Символ-Плюс, 2002. — 544 с.
30. Машнин Т. Современные Java-технологии на практике. — СПб.: БХВ-Петербург,2010. — 560 с.
31. Гери Д. М., Хорстманн К. С. JavaServer Faces. Библиотека профессионала. —3-е изд. — М.: Вильямс, 2011. 544 с.
32. Кэй М. XSLT. Справочник программиста. — СПб.: Символ-Плюс, 2002. — 1016 с.
33. Технічна документація мови JavaScript [Електронний ресурс] / – Режим доступу до ресурсу: https://learn.javascript.ru/
34. Технічна документація React.js [Електронний ресурс] / – Режим доступу до ресурсу: https://devdocs.io/react/
35. Технічна документація npm [Електронний ресурс] / – Режим доступу до ресурсу: https://docs.npmjs.com/

36. Технічна документація Node.js [Електронний ресурс] / – Режим доступу до ресурсу: https://nodejs.org/dist/latest-v12.x/docs/api/
37. Руководство по языку программирования Java [Електронний ресурс]. /– Режим доступу до ресурсу: https://metanit.com/java/tutorial/
38. Руководство по React [Електронний ресурс]. /– Режим доступу до ресурсу: https://metanit.com/web/react/
39. Руководство по Typescript [Електронний ресурс]. /– Режим доступу до ресурсу: https://metanit.com/web/typescript/
40. Онлайн-руководство по MongoDB [Електронний ресурс]. /– Режим доступу до ресурсу: https://metanit.com/nosql/mongodb/
41. Design Patterns [Електронний ресурс]. /– Режим доступу до ресурсу: https://howtodoinjava.com/gang-of-four-java-design-patterns/
42. Java Best Practices Guide [Електронний ресурс]. /– Режим доступу до ресурсу: https://howtodoinjava.com/java-best-practices/
43. Introduction to MongoDB: Why MongoDB? [Електронний ресурс]. /– Режим доступу до ресурсу: https://howtodoinjava.com/mongodb/introduction-to-mongodb-why-mongodb/
44. REST Resourse Naming Guide [Електронний ресурс]. /– Режим доступу до ресурсу: https://restfulapi.net/resource-naming/
45. Typescript Tutorial [Електронний ресурс]. /– Режим доступу до ресурсу: https://howtodoinjava.com/typescript/typescript-tutorial/

ДОДАТОК 1

Реалізація використання блокчейн-технологій у енергетичному секторі

СПЕЦИФІКАЦІЯ

УКР.НТУУ«КПІ ім. Ігоря Сікорського»_ТЕФ_АПЕПС_ТМ62203_20Б

Аркушів 2

Київ 2020

Позначення	Найменування	Примітки
Документація		
УКР.НТУУ«КПІ ім. Ігоря Сікорського»_ТЕФ_АПЕПС_ТМ62203_20Б	Записка.docx	Текстова частина дипломної роботи
УКР.НТУУ«КПІ ім. Ігоря Сікорського»_ТЕФ_АПЕПС_ТМ62203_20Б	Діаграми.vsdx	UML діграми
Компоненти		
УКР.НТУУ«КПІ ім. Ігоря Сікорського»_ТЕФ_АПЕПС_ТМ62203_20Б	blockchain_protoype .jar	Прототип блокчейну

ДОДАТОК 2

Реалізація використання блокчейн-технологій у енергетичному секторі

ТЕКСТ ПРОГРАМНОГО МОДУЛЮ

УКР.НТУУ«КПІ ім. Ігоря Сікорського»_ТЕФ_АПЕПС_ТМ62203_20Б

Аркушів 7

Київ 2020

Текст програми

```
import com.google.gson.annotations.Expose;
import lombok.Data;

import java.nio.charset.StandardCharsets;
import java.security.*;
import java.util.Date;

@Data
public class Transaction {
    private PublicKey from;
    private PublicKey to;
    private int amount;
    private long timestamp;
    private byte[] signature;
    private String hash;

    public Transaction(User from, User to, int amount) {
        this.from = from == null ? null : from.getAddress();
        this.to = to == null ? null : to.getAddress();

        this.amount = amount;
        this.timestamp = new Date().getTime();

        hash = calculateHash();
    }

    public String calculateHash() {
        return from == null
                ? Util.createHash(to.toString() + amount + timestamp)
                : Util.createHash(from.toString() + to.toString() + amount + timestamp);
    }

    public boolean isTransactionValid() {
        return from != null && to != null && amount > 0;
    }

    public void sign(User user) throws NoSuchAlgorithmException, InvalidKeyException, SignatureException {
        if (isTransactionValid()) {
            Signature signature = Signature.getInstance("SHA256WithDSA");
            SecureRandom secureRandom = new SecureRandom();

            signature.initSign(user.getPrivateKey(), secureRandom);
            signature.update(hash.getBytes(StandardCharsets.UTF_8));

            this.signature = signature.sign();
        }
    }

    public boolean isSignVerified() throws NoSuchAlgorithmException, InvalidKeyException, SignatureException {
        if (isTransactionValid()) {
            Signature signature = Signature.getInstance("SHA256WithDSA");
            signature.initVerify(from);
            byte[] bytes = hash.getBytes(StandardCharsets.UTF_8);

            signature.update(bytes);

            return signature.verify(this.signature);
        }
```

```
        return false;
    }
}

import lombok.Data;

import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.SignatureException;
import java.util.ArrayList;
import java.util.Date;
import java.util.List;

@Data
public class Block {
    private String hash;
    private String previousHash;
    private long timeStamp;
    private int nonce;
    private List<Transaction> transactions;

    public Block(String previousHash, List<Transaction> pendingTransactions) {
        this.previousHash = previousHash;
        this.timeStamp = new Date().getTime();
        this.transactions = pendingTransactions != null ? new ArrayList<>(pendingTransactions) : new ArrayList<>();

        this.hash = calculateHash();
    }

    public String calculateHash() {
        return Util.createHash(previousHash +
                timeStamp +
                nonce +
                transactions
        );
    }

    public void mineBlock(int difficulty) {
        String target = new String(new char[difficulty]).replace('\0', '0');

        while (!hash.substring(0, difficulty).equals(target)) {
            nonce++;
            hash = calculateHash();

        }

        System.out.println("Block has mined with hash = " + hash);
    }

    public boolean hasValidTransactions() throws NoSuchAlgorithmException, InvalidKeyException, SignatureException {
        for (Transaction transaction : transactions) {
            if (!transaction.isTransactionValid() && !transaction.isSignVerified()) {
                return false;
            }
        }

        return true;
    }
}

import com.google.gson.GsonBuilder;
import lombok.Data;
```

```
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.SignatureException;
import java.util.ArrayList;
import java.util.List;

@Data
public class Blockchain {
    private List<Block> chain;
    private int difficulty;
    private List<Transaction> pendingTransactions;
    private int miningReward;

    public Blockchain(int difficulty, int miningReward) {
        this.difficulty = difficulty;
        this.chain = new ArrayList<>();
        this.pendingTransactions = new ArrayList<>();
        this.miningReward = miningReward;

        createGenesisBlock();
    }

    private void addBlock(Block newBlock) {
        newBlock.mineBlock(difficulty);
        chain.add(newBlock);
    }

    public Block getLatestBlock() {
        return chain.get(chain.size() - 1);
    }

    public void createGenesisBlock() {
        Block genesisBlock = new Block("0", null);
        genesisBlock.mineBlock(difficulty);

        chain.add(genesisBlock);
    }

    public boolean isChainValid() throws NoSuchAlgorithmException, InvalidKeyException, SignatureException {
        boolean checkingResult = true;

        for (int i = 1; i < chain.size(); i++) {
            Block currentBlock = chain.get(i);

            if (!currentBlock.hasValidTransactions()) {
                return false;
            }

            checkingResult = currentBlock.getHash().equals(currentBlock.calculateHash());
        }

        return checkingResult;
    }

    public void minePendingTransactions(User rewarderAddress, User minerRewardAddress) throws
NoSuchAlgorithmException, InvalidKeyException, SignatureException {
        Transaction rewardTx = new Transaction(rewarderAddress, minerRewardAddress, miningReward);
        rewardTx.sign(rewarderAddress);
        pendingTransactions.add(rewardTx);

        Block newBlock = new Block(getLatestBlock().getHash(), pendingTransactions);
```

```
        addBlock(newBlock);

        pendingTransactions.clear();
    }

    public void addTransaction(Transaction transaction) {
        if (transaction.isTransactionValid()) {
            pendingTransactions.add(transaction);
        }
    }

    @Override
    public String toString() {
        return new GsonBuilder()
                .setPrettyPrinting()
                .registerTypeAdapter(Blockchain.class, new BlockchainSerializer())
                .create()
                .toJson(this);
    }
}

import java.nio.charset.StandardCharsets;
import java.security.*;

public class Util {
    public static String createHash(String input) {
        try {
            MessageDigest digest = MessageDigest.getInstance("SHA-256");

            byte[] hash = digest.digest(input.getBytes(StandardCharsets.UTF_8));
            StringBuilder hexString = new StringBuilder();

            for (byte hash1 : hash) {
                String hex = Integer.toHexString(0xff & hash1);

                if (hex.length() == 1) {
                    hexString.append('0');
                }
                hexString.append(hex);
            }

            return hexString.toString();
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }
}

import lombok.Data;

import java.security.*;

@Data
public class User {
    private PublicKey address;
    private PrivateKey privateKey;
    private int balance;

    public User() {
        balance = 0;
    }
```

```
    public void generateKeys() throws NoSuchAlgorithmException {
        if (address != null && privateKey != null) {
            return;
        }

        KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance("DSA");
        KeyPair keyPair = keyPairGenerator.generateKeyPair();

        address = keyPair.getPublic();
        privateKey = keyPair.getPrivate();
    }

    public void processNewTransactions(Block lastBlock) {
        for (Transaction transaction : lastBlock.getTransactions()) {
            processTransaction(transaction);
        }
    }

    public void processTransaction(Transaction transaction) {
        if (transaction == null) {
            return;
        }

        if (transaction.getTo().equals(address)) {
            balance += transaction.getAmount();
        }

        if (transaction.getFrom().equals(address)) {
            balance -= transaction.getAmount();
        }
    }
}

import org.bouncycastle.jce.provider.BouncyCastleProvider;

import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.Security;
import java.security.SignatureException;

public class Main {
    public static void main(String[] args) throws NoSuchAlgorithmException, SignatureException, InvalidKeyException {
        Security.addProvider(new BouncyCastleProvider());

        Blockchain blockchain = new Blockchain(2, 1);

        User user1 = new User();
        User user2 = new User();
        User rewarder = new User();
        User miner = new User();

        user1.generateKeys();
        user2.generateKeys();
        rewarder.generateKeys();
        miner.generateKeys();

        Transaction transaction = new Transaction(user1, user2, 50);
        Transaction oneMoreTransaction = new Transaction(user1, user2, 70);

        Transaction transactionAgain = new Transaction(user2, user1, 11);

        transaction.sign(user1);
```

```
        oneMoreTransaction.sign(user1);
        transactionAgain.sign(user2);

        blockchain.addTransaction(transaction);
        blockchain.addTransaction(oneMoreTransaction);

        blockchain.minePendingTransactions(rewarder, miner);

        user1.processNewTransactions(blockchain.getLatestBlock());
        user2.processNewTransactions(blockchain.getLatestBlock());
        miner.processNewTransactions(blockchain.getLatestBlock());
        rewarder.processNewTransactions(blockchain.getLatestBlock());

        blockchain.addTransaction(transactionAgain);

        blockchain.minePendingTransactions(rewarder, miner);

        user1.processNewTransactions(blockchain.getLatestBlock());
        user2.processNewTransactions(blockchain.getLatestBlock());
        miner.processNewTransactions(blockchain.getLatestBlock());
        rewarder.processNewTransactions(blockchain.getLatestBlock());

//      System.out.println(blockchain.isChainValid());

//      System.out.println(user1.getBalance());
//      System.out.println(user2.getBalance());
//      System.out.println(rewarder.getBalance());
//      System.out.println(miner.getBalance());

        System.out.println(blockchain);
    }
}
```

ДОДАТОК 3

Реалізація використання блокчейн-технологій у енергетичному секторі

ОПИС ПРОГРАМНОГО МОДУЛЮ

УКР.НТУУ«КПІ ім. Ігоря Сікорського»_ТЕФ_АПЕПС_ТМ62203_20Б

Аркушів 9

Київ 2020

АНОТАЦІЯ

Додаток містить опис системи, для обліку та торгівлі енергоресурсами.

В додатку виконуються такі функції:

— введення вхідних даних для авторизації, обліку та продажу енергоресурсів ;

— робота з блокчейном;

— переведення криптовалюти**.**

Вхідні та вихідні дані отримуються через форми, реалізованими засобами React.js у вигляді окремого сервера для роботи з користувачем.

Робочий сервер виконано мовою Javascript з використанням технології Node.js. Робочий сервер окремо підключається до репліки бази MongoDB.

ЗМІСТ

ЗАГАЛЬНІ ВІДОМОСТІ

У цьому додатку описано прототип системи з використанням алгоритмів блокчейну.

Модулі системи надано в ДОДАТКУ 2.

Розроблений додаток працює в операційних системах Windows7, Windows8, Windows10, Unix.

Компоненти необхідні для установки прототипу: JVM.

Використана мова програмування для прототипу — Java.

Компоненти необхідні для установки системи: NPM, Node.js, React.js.

Використана мова програмування для системи— Javascript.

ФУНКЦІОНАЛЬНЕ ПРИЗНАЧЕННЯ

Розроблений прототип демонструє процес роботи блокчейну.

Розроблений прототип являється концепцією, яка закладена в роботі автоматизованої системи з обліку енергоресурсів на основі блокчейн технології. Імплементова автоматизована система дозволяє проводити обмін енергоресурсів на криптовалюту. Система може бути використана керівниками підприємств та особам, яким необхідно здійснювати оплату енергоресурсів.

ОПИС ЛОГІЧНОЇ СТРУКТУРИ

Автоматизована система розроблена на основі прототипу являє собою робочий сервер для безпосередньої роботи з блокчейном та окремий сервер, що надає графічний інтерфейс користувача. Для роботи з блокчейном, кожен користувач повинен мати на своїй локальній машині цей сервер та базу репліку бази даних. Комунікація здійснюється від сервера графічного інтерфейсу до робочого сервера і до бази даних. Окрім того, робочі сервера в рамках мережі комунікують один із одним.

ВИКОРИСТОВУВАНІ ТЕХІЧНІ ЗАСОБИ

Компоненти необхідні для установки прототипу: JVM.

Використана мова програмування для прототипу— Java.

Компоненти необхідні для установки системи: NPM, Node.js, React.js.

Використана мова програмування для автоматизованої системи— Javascript.

Розроблена автоматизована система працює в операційних системах Windows7, Windows8, Windows10 та потребує встановлення компонентів: NPM, Node.js, MongoDB.

ВИКЛИК І ЗАВАНТАЖЕННЯ

Для запуску серверів необхідно викликати shell команди і дочекатися запуску серверів. Після цього необхідно в браузері перейти за адресою зворотньої петлі (127.0.0.1) із вказанням порту на головну сторінку з подальшою реєстрацією нового або авторизацією вже існуючого користувача.

ВХІДНІ І ВИХІДНІ ДАНІ

Вхідні дані представлені у вигляді текстового або цифрового значення в залежності від призначення форми. Вхідні дані вводяться та зчитуються із засобів мови HTML5, логіка обробки даних здійснюється за допомогою мови Javascript.

Вихідні дані представлені у вигляді текстового або цифрового значення, обернені у формат JSON та збережені в репліках баз даних користувачів.

Вихідні дані отримуються з бази даних і представляються користувачам у текстовому або цифровому вигляді.

ДОДАТОК 4

Реалізація використання блокчейн-технологій у енергетичному секторі

ТЕКСТ ТЕЗИ КОНФЕРЕНЦІЇ

УКР.НТУУ«КПІ ім. Ігоря Сікорського»_ТЕФ_АПЕПС_ТМ62203_20Б

Аркушів 5

Київ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

СУЧАСНІ ПРОБЛЕМИ НАУКОВОГО ЗАБЕЗПЕЧЕННЯ ЕНЕРГЕТИКИ

Матеріали XVIII Міжнародної науково-практичної конференції молодих вчених і студентів 2020 року

ТОМ 2

Київ- 2020

УДК 620.9(062)+621.311(062)
С91

Сучасні проблеми наукового забезпечення енергетики: Матеріали XVIII Міжнародної науково-практичної конференції молодих вчених і студентів 2020 року. У 2 т. – К. : 7 КПІ ім. Ігоря Сікорського, 2020. – Т. 2. – 160 с.

ISBN 978-966-622-997-0
ISBN 978-966-622-999-4 (Т.2)

Подано тези доповідей XVIII Міжнародної науково-практичної конференції молодих вчених і студентів «Сучасні проблеми наукового забезпечення енергетики» за напрямами: автоматизація теплоенергетичних процесів, геометричне моделювання та проблеми візуалізації, програмне забезпечення інформаційних систем та мережних комплексів, моделювання та аналіз теплоенергетичних процесів, сучасні проблеми сталого розвитку енергетики.

Друкується в авторській редакції за рішенням Вченої ради теплоенергетичного факультету Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (протокол № 9 від 29 квітня 2020 р.)

ISBN 978-966-622-997-0
ISBN 978-966-622-999-4 (Т.2)

УДК 342.951

Студент 4 курсу, гр. ТМ-62 Локотарьов Є.О.
Доц., к.е.н. Сегеда І.В.

БЛОКЧЕЙН - РЕГУЛЯТОР ПРОСУВАННЯ ЦИФРОВОЇ ЕКОНОМІКИ В ЕНЕРГЕТИЦІ

Розвиток ІТ-технологій щодня пропонує світові нові інструменти для оптимізації бізнес-процесів. Одним з останніх таких інструментів є технологія – блокчейн.

Думки експертів щодо ідеї впровадження криптовалют розділилися: одні вважають це справді революційним, але не зовсім зрозуміло, чи вдасться здійснити цю революцію. Другі - це інновації, які потребують значної адаптації. Тому питання подолання певної багатозначності практичного використання є актуальними, та потребують подальшого дослідження [1].

В сучасних умовах прийнята технологія обліку і контролю енергоресурсів застаріла через організаційну та технічну недосконаліть структур, що здійснюють облік. Ці проблеми стають причиною постійних збитків, що явно свідчить про необхідність створення сучасної автоматизованої системи..

Блокчейн - це система, яка дозволяє організувати однорангову взаємодію в мережі без посередників і прямим доступом до інформації всім учасникам мережі [2]. Завдяки своїй структурі і принципу роботи, в системі неможлива підробка даних (тому що для підробки необхідно буде використовувати колосальні обчислювальні ресурси, які в кінцевому результаті не зможуть окупитися).

Блокчейн складається з блоків; блоки із основної концепції даної технлогії – транзакцій. Саме транзакції і здійснюють зміни в системі і несуть корисну інформацію.

Переваги системи з обліку енергоресурсів на основі технології блокчейн:

1. Низькі витрати на збереження і забезпечення безпеки даних;
2. Безпосередній зв'язок від виробника до споживача;
3. Прозорий і простий моніторинг виробництва та споживання енергоресурсів;
4. Гнучкість у регулюванні навантажень та постачань.

Слід зазначити, що концепція блокчейну гнучка та розширювана по своїй суті. Це дозволяє робити носієм корисної інформації не лише спожиті або надані енергоресурси, але і зобов'язання. Іншими словами, це дозволить постачальникам та продавцям енергоресурсів [3]:

1. Застосовувати систему для керування пристроями, що підключені до Інтернету;
2. Надасть можливість формувати та підписувати контракти (смарт-контракт);
3. Формувати квоти на викиди шкідливих речовин;
4. Сертифікувати виробництво відновлювальних джерел енергії;
5. Формувати рахунки за спожиту енергію з можливістю їх моментальної сплати.

Перелік посилань:

1. Сегеда І.В., Локотарев Є.О., Шаповал В.О. Реалізація використання блокчейн-технологій у енергетичному секторі. / Вчені записки Таврійського національного університету імені В.І. Вернадського Серія:Економіка і управління Том 30 (69). № 4, 2019, С. 160-165 (DOI: https://doi.org/10.32838/2523-4803/69-4-51)
2. Nakamoto S. A Peer-to-Peer Electronic Cash System [Електронний ресурс] // Bitcoin. – Режим доступ до ресурсу: https://bitcoin.org/bitcoin.pdf
3. Цифровая энергетика: видение, практики, технологии : Информационно-аналитические работы 2018 г. / Инфраструктурный Центр EnergyNet. — [б. м.] : [б. и.], 2018. — 224 с.

ДОДАТОК 5

Реалізація використання блокчейн-технологій у енергетичному секторі

ТЕКСТ НАУКОВОЇ СТАТТІ

УКР.НТУУ«КПІ ім. Ігоря Сікорського»_ТЕФ_АПЕПС_ТМ62203_20Б

Аркушів 10

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В.І. ВЕРНАДСЬКОГО

Журнал заснований у 1918 році

ВЧЕНІ ЗАПИСКИ

ТАВРІЙСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ В.І. ВЕРНАДСЬКОГО

Серія: Економіка і управління

Том 30 (69). № 4, 2019

Частина 2

Київ
2019

Науковий журнал

ВЧЕНІ ЗАПИСКИ
ТАВРІЙСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ В.І. ВЕРНАДСЬКОГО

Серія: Економіка і управління

Том 30 (69). № 4, 2019
Частина 2

Коректура • *О. Скрипченко*

Комп'ютерна верстка • *В. Удовиченко*

Адреса редакції:
Таврійський національний університет імені В.І. Вернадського
м. Київ, вул. Івана Кудрі, 33
Телефон редакції: +38 (095) 430 01 12
Електронна пошта: editor@econ.vernadskyjournals.in.ua
Сторінка журналу: www.econ.vernadskyjournals.in.ua

Формат 60x84/8. Гарнітура Times New Roman.
Папір офсетний. Цифровий друк. Обл.-вид. арк. 19,14. Ум. друк. арк. 20,23.
Підписано до друку 27.09.2019. Замов. № 0919/198. Наклад 150 прим.

Видавництво і друкарня – Видавничий дім «Гельветика»
73034, м. Херсон, вул. Паровозна, 46-а, офіс 105
Телефон +38 (0552) 39 95 80
E-mail: mailbox@helvetica.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 6424 від 04.10.2018 р.

Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління

8. МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

DOI: https://doi.org/10.32838/2523-4803/69-4-51

УДК 336. 621

Сегеда І.В.
кандидат економічних наук, доцент,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Локотарев Є.О.
бакалавр,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Шаповал В.О.
бакалавр,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Segeda Irina, Lokotariev Eugene, Shapoval Vitaliy
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

РЕАЛІЗАЦІЯ ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У ЕНЕРГЕТИЧНОМУ СЕКТОРІ

У статті проаналізовано процеси входження криптовалют в енергетичний сектор, питання подолання певної багатозначності їх віртуального та практичного використання. Автори концептуалізують цей процес як цифрову блокчейн-революцію. Зазначено, що блокчейн є механізмом верифікації транзакцій у мережі, підвищує довіру клієнтів і дає змогу позбутися посередників у фінансових операціях. Показано потенційні переваги «розумних контрактів», які здатні не тільки змінити технологічний уклад, але й повністю змінити взаємини суб'єктів суспільства, а також взаємини між суспільством і державою. Розглянуто децентралізовану модель енергетичних транзакцій та енергопостачання. Представлено головні тренди блокчейну в енергетиці. Запропоновано алгоритм системи обліку споживання та оплати платежів за енергоресурси як блокчейн-додаток, який буде реалізовувати одноранговy взаємодію між користувачами.

Ключові слова: *криптовалюта, блокчейн, блокчейн-технології, смарт-контракт, децентралізована модель, енергетичні транзакції.*

Постановка проблеми. Розвиток IT-технологій щодня пропонує світу нові інструменти для оптимізації бізнес-процесів. Одним з останніх таких інструментів є технологія блокчейну (blockchain technology).

Думки експертів про ідею впровадження криптовалют розділилися: одні вважають це справді революційним, але не зовсім розуміють, чи вдасться здійснити цю революцію, а інші називають це інноваціями, які потребують значної адаптації та не є революційними. Отже, питання подолання певної багатозначності їх віртуального й практичного використання є актуальними та потребують подальшого дослідження.

В сучасних умовах прийнята технологія обліку й контролю енергоресурсів застаріла через організаційну та технічну недосконалість структур, що здійснюють облік. Ці проблеми стають причиною постійних збитків, що явно свідчить про необхідність створення сучасної автоматизованої системи.

Аналіз останніх досліджень і публікацій. Найвідоміша робота з технології блокчейну датується 2008 роком. Її автором є Сатоші Накамото [1], що описує технічні рішення, які використовуються в проектах Bitcoin і Blockchain. Одночасно в документі з'явилися терміни "bitcoin" та "blockchain", які досі часто плута-

ють. Вперше технологія блокчейну була впроваджена у 2009 році як інструмент проведення операцій з біткоїнами в електронній валюті, тобто вона була спільним реєстром транзакцій. Нині блокчейн-технологія розвивається як автономна технологія, яку можна використовувати поза системами криптовалют. Ден Тапскотт і Алекс Тапскотт, що є авторами публікацій з блокчейну, проаналізували програми, послуги, бізнес-моделі, ринки, організації та навіть уряди, які керують блокчейном. Визначено закономірності, сформульовано сім принципів, на які покладаються послідовники технологій [2].

Формулювання цілей статті. Метою статті є систематизація інформації про технологію блокчейну, аналіз її перспектив та варіантів використання в енергетиці, вивчення основних блокчейн-тенденцій в енергетиці, розгляд алгоритму системи обліку споживання та платежів за енергоресурси.

Виклад основного матеріалу. Енергетичний сектор перебуває на стадії переходу від централізованого ринку до децентралізованого, оцифрованого сектору, в якому люди та компанії можуть досягти повної автономії шляхом виробництва та зберігання енергії.

Парадигма на поточне десятиліття, яка спирається на розрахунки, засновується на криптографії блокчейну. На наш погляд, це є процесом цифрової блокчейн-революції. Революційний потенціал блокчейн-технологій буде розвиватись та впроваджуватись досить швидко завдяки наявності Інтернету та мобільного зв'язку. Блокчейн стає невіддільним економічним шаром Інтернету. Реалізований функціонал в процесі цифрової блокчейн-революції – це повноцінний економічний шар, якого в Інтернеті ще не було. На інтегрованому фізичному рівні перебувають розрахунки з багатьма пристроями, на вершині яких є шар для оброблення таких платежів, як мікроплатежі, децентралізована біржа, заробіток та витрати токенів, отримання та передача цифрових активів, створення та виконання смарт-контрактів. Простіше кажучи, якщо ця революційна технологія буде впроваджена у повсякденне життя, тоді контроль над банками, державними установами, аудиторами, регуляторами, страховими компаніями чи реєстраторами просто не знадобиться. Сьогодні блокчейн дає змогу трансформувати цілі галузі економіки й економити великі кошти.

Нині існують три концепції, цілі та перспективи є різними, але вони мають одну технологічну базу та учасників [3].

Криптовалюта передбачає мінімізацію потреби в довірі, адже її концепція полягає у здійсненні безпечних операцій без централізованого контролю. Блокчейн-трекінг передбачає, що учасники мережі можуть приймати спільне рішення щодо інформації, яка перебуває в межах довіри. Криптоактиви відповідають за торгівлю, адже ця концепція передбачає, що віртуальні валюти можуть бути фінансовими інструментами та використовуватися як продані активи.

Слід зазначити, що вони не є взаємовиключними.

Автори зосереджуються на використанні технології блокчейну. У звіті Всесвітнього економічного форуму (ВЕФ) наведено таке визначення технології "blockchain", або технології розподіленого реєстру (distributed ledger technology, DLT): технологічний протокол, що дає змогу обмінюватися даними безпосередньо між різними сторонами в мережі, не потребуючи посередників [4]. Учасники мережі зв'язуються із зашифрованими ідентифікаторами (анонімно), а потім кожна транзакція додається до незмінного ланцюга транзакцій і розподіляється по всіх мережевих вузлах.

Через активний розвиток технології "blockchain" «розумні контракти» замінили звичайні контракти. «Розумні контракти» (смарт-контракти) – це одне із застосувань блокчейну, яке викликає найбільший інтерес. «Розумний контракт» – це договір між двома сторонами, що зберігається в блокчейні. Такі договори можуть укладатися між двома людьми, (P2P), людиною та організацією (P2O), людиною та машиною (P2M). «Розумні контракти» дають змогу автоматизувати виплати та перекази валют чи інших активів відповідно до встановлених умов. Як тільки умова, зазначена у смарт-договорі, виконується, договір укладається автоматично, відбувається обмін активами (готівкою, цифровою валютою, правом власності) між сторонами, які домовляються. Потім транзакція реплікується та перевіряється у ланцюзі блоків. «Розумні контракти» дають змогу обмінятися активами, якщо треті сторони не знають про передачу. Це відкриває можливість створення нової форми віртуального контракту. Однак через фрагменти коду, які автоматично виконують дії за певних умов, «розумні договори» ще не можуть конкурувати зі звичайними контрактами. Проте вони можуть бути використані як доказ розв'язання конкретної задачі [5].

Назвемо можливості використання блокчейну в енергетичній галузі. Блокчейн-технологія здатна докорінно змінити енергетичну систему спочатку шляхом трансформації окремих секторів, а потім шляхом трансформації всього ринку електроенергії.

Міжнародні енергетичні компанії розробляють проекти, які надалі з'єднають усіх споживачів в одну мережу, тобто децентралізовану систему. За допомогою «розумних контрактів» буде спрощена наявна багаторівнева система, що складається з виробників електроенергії, операторів розподільної мережі, операторів-постачальників, постачальників платіжних послуг банківських послуг, споживачів та трейдерів. Усі транзакції щодо отримання енергії та оплати за неї здійснюватимуться безпосередньо в мережі, об'єднуючи рівних учасників, тобто споживачів та виробників енергії. Завдяки цьому електроенергія буде дешевою.

Крім того, всі транзакції будуть відкритими. Люди не зможуть прострочити платіж за споживання енергії, адже «розумний контракт» контролюватиме виконання всіх операцій. Система сама заплатить за себе, тобто спише стільки криптовалюти, скільки вам знадобиться для транзакції з передачі енергії.

Моделі транзакцій на блокчейні базуються на тому, що вся електроенергія, що подається в електромережу, може бути чітко віднесена до обліку конкретних спо-

живачів за короткий проміжок часу. Це означає, що розрахунок за всю вироблену та спожиту електроенергію може бути дуже точно проведений за змінними цінами. Електрика буде продовжувати надходити до кінцевого споживача безпосередньо від найближчого виробника електроенергії. База даних, що зазнала значного поліпшення, дасть змогу точно «налаштувати» операції в мережі як на рівні передачі електроенергії, так і на рівні розподілу. Спрощений процес взаєморозрахунків приведе до зниження обсягу балансу енергії, рахунки на яку виставляються учасникам ринку.

Завдяки блокчейну всі потоки електроенергії захищені від сторонніх маніпуляцій. Це дасть змогу сертифікувати електроенергію, перевірити квоти на допустимі викиди, кількість яких регулюється законодавством. Децентралізована технологія функціонує як база даних транзакцій, побудована за принципом розподіленого реєстру, тому за допомогою блокчейну можна створити універсальний архів для зберігання всіх даних за виставленими рахунками за електроенергію. Споживачі отримають можливість розширеного контролю за своїми договорами на постачання електроенергії, а також дані про споживання електроенергії. Всі записи зберігатимуться у відкритому доступі в блокчейн-реєстрі, який буде коригувати всі питання права власності та поточний стан активів, тобто розумних інтернет-речей (Інтернет речей, IoT).

Технологія блокування не тільки використовується для проведення операцій з постачання енергії, але й може слугувати основою для процесів вимірювання кількості споживаної електроенергії, виставлення рахунків за споживання кількості та проведення розрахунків. Інші можливі додатки включають право власності на активи, управління активами, систему сертифікатів гарантованого походження, квоти на викиди вуглекислого газу та сертифікати, що підтверджують виробництво електроенергії на основі використання відновлюваних джерел енергії (ВДЕ). Можливості використання технологій в енергетиці представлені в табл. 1.

Під час об'єднання окремих блокчейн-додатків у майбутньому може з'явитися децентралізована система енергетичних транзакцій та постачання енергії. Постачання електроенергії, виробленої на об'єктах малої енергетики, кінцевим споживачам здійснюватиметься через мікромережі. Кількість виробленої та спожитої електроенергії вимірюватиметься за допомогою розумних лічильників, а операції з торгівлі енергією та сплата криптовалютою контролюватимуться за допомогою смарт-контрактів та здійснюватимуться з використанням блокчейну.

Слід зазначити, що наявні блокчейн-додатки можна розділити на такі три великих категорії залежно від рівня розроблення, як блокчейн-додатки версій 1.0, 2.0 та 3.0. Технологія блокчейну нового покоління, тобто блокчейн 3.0, ще розробляється. Blockchain 3.0 – це етап розвитку технологій, на якому здійснюється подальший розвиток концепції «розумного контракту» задля створення децентралізованих, автономних організаційних підрозділів, які керуються власними законами та працюють майже незалежно. Децентралізована система енергетичних транзакцій та постачання енергії представлена на рис. 1.

Прозоре та децентралізоване врегулювання угод на вітчизняному енергетичному ринку збільшить частку електроенергії, отриманої від відновлюваних джерел енергії.

Блокчейн чітко фіксує джерело походження кожної кіловат-години в загальній мережі й дає покупцю гарантію, що він отримає енергію вітру, а не енергію, згенеровану газовою станцією.

Отже, доцільно поєднувати нову технологічну систему з інноваційною ідеєю та блокчейн-технологією в тих установках, які генерують «зелену» енергію, тобто екологічно чисту й невичерпну за людськими мірками енергію сонця, вітру, місяця, води, гейзерів тощо. Для адаптації відновлюваних джерел енергії до повсякденного життя необхідно автоматизувати систему за допомогою спеціального обладнання нового типу [6].

Назвемо основні тренди технологій блокчейну в енергетиці.

1)Вихід на ринок блокчейн-технологій компаній гігантів. Партнери-засновники "Rocky Mountain Institute" та "Grid Singularity" мають намір створити нову платформу для торгівлі енергоресурсами на основі блокчейну (Енергетична веб-платформа), яка забезпечує функціонал, необхідний для реалізації різних варіантів використання в енергетичному секторі.

2)Знищення оптового ринку електроенергії. Компанія "Ponton" має на меті створення першого розподіленого оптового ринку для позабіржової торгівлі

Таблиця 1

Різні варіанти використання блокчейну в енергетиці

Транзакції та «розумні контракти»	Права власності на активи та управління ними	Децентралізовані інформаційні системи
Децентралізована торгівля електроенергією	Реєстрація власності та ведення реєстру активів	Облік електроспоживання та виставлення рахунків за електроенергію
Особливі можливості для просьюмерів	«Зелені» сертифікати	Облік споживання тепла та виставлення рахунків за нього
Впровадження криптовалюти	Квоти на викиди вуглекислого газу, сертифікація виробництва електроенергії на основі відновлюваних джерел енергії	Оплата зарядки електромобілів
Зарядка електромобілів		
Управління розумними пристроями в Інтернеті речей		

Рис. 1. Децентралізована система енергетичних транзакцій та енергопостачання

оптовою енергетичної продукцією за допомогою свого проекту "Enerchain".

3)Підвищення енергоефективності. У Німеччині проект працює з компанією "Sonnen", щоби використовувати склад як буфер для поглинання перевантажень електроенергії від вітроелектростанцій. Ця система виявилась корисною для зменшення витрат на скорочення вітрогенераторів.

4)Торгівля енергією за допомогою токенів. Проекти спрямовані на використання блокчейну для забезпечення торгівлі електроенергією. Проекти створюють ринок локально генерованої електроенергії, "Grid+" зосереджується більше на зниженні роздрібних цін на енергоносії, тоді як "Power Ledger" зосереджується на створенні ринку надлишкової енергії [7].

5)Розвиваючі стартапи. Згідно з даними "Reuters" енергетичні блокчейн-стартапи зібрали близько 200 мільйонів доларів завдяки "Initial coin offering" у 2018 році. Згідно з даними провайдера даних ринку "PitchBook" венчурні інвестиції капіталу в криптовалюти та блокчейн-стартапи встановлять новий рекорд у 2019 році.

Необхідно звернути увагу на проблему обліку споживання та збирання платежів за енергоресурси. Технологія обліку й контролю енергоресурсів, яка сьогодні застосовується, завдає шкоди суб'єктам господарювання, які її використовують. Головною причиною є організаційна й технічна недосконалість структур, які здійснюють облік. Ці проблеми стають причиною постійних збитків, що свідчить про необхідність створення сучасної автоматизованої системи.

Авторами розроблено алгоритм системи обліку споживання та платежів за енергоресурси, на основі якого буде розроблена автоматизована система.

Планується створити додаток, який буде реалізовувати однорангову взаємодію між користувачами (один з них буде оплачувати рахунки за енергоресурси, другий буде, власне, надавати ці енергоресурси). Той, хто оплачує використання енергоресурсів, водночас зможе надавати їх (наприклад, людина платить за газ, але у неї стоїть вітряна електростанція, тому надлишок виробленої електроенергії вона продає в мережу).

Додаток буде мати два типи серверів.

1)Сервер, який буде працювати тільки з блокчейном. Блокчейн з усіма транзакціями буде зберігатись в нереляційній базі даних (БД). Сервер буде проводити валідацію транзакцій і всього ланцюжка, здійснювати переказ криптовалюти (планується вводити свою криптовалюту, якою сплачуватимуться рахунки). Якщо брати як приклад систему «Біткоїн», то кожному користувачу встановлюється на ПК програма, яка зберігає ланцюжок і надає функціонал для роботи з нею. В нашому випадку кожному користувачу планується розгортати вузол (екземпляр сервера) в кластері з окремою БД. Іншими словами, інфраструктура буде представлена децентралізованою системою серверів.

2)Сервер, який буде надавати функціонал користувача. Всі дані будуть зберігатися в реляційній БД. Планується розгорнути один сервер, який буде давати можливість працювати зі своїми рахунками й контрактами. З іншого боку, можна сказати, що цей сервер буде проміжною ланкою між користувачами, а його основним завданням буде комунікація між користувачами.

– Користувачі зможуть вручну вносити показання лічильників (можна ще зробити заглушку, яка буде імітувати роботу лічильника, який автоматично вносить на рахунок показники за використані енергоресурси).

– Користувачі зможуть здійснювати оплату рахунків за енергоресурси.

– Користувачі зможуть бачити різноманітну статистику за надані (якщо користувач надає енергоресурси) і, відповідно, спожиті енергоресурси (якщо він їх споживає).

– Можна імітувати інтеграцію з банківськими сервісами (перетворення паперових грошей на криптовалюту, яка буде використовуватися в додатку). В реальних умовах лічильники мають можливість спілкуватись із сервером і передавати йому свідчення за використані енергоресурси.

Наведемо алгоритм роботи блокчейну.

Ланцюжок складається з набору блоків. Кожен блок зберігає в собі транзакції. Транзакція містить публічний ключ (адресу гаманця) відправника й одержувача. Також у транзакції зберігаються грошова сума, яку відправник передає одержувачу, та інформація про транзакції, яку заповнює користувач або сама система.

Користувач має також приватний ключ, яким підписує транзакції, говорячи «Це мій переказ грошей». Приватний ключ доступний тільки користувачу, тому ніхто, крім нього, не має до нього доступу. За допомогою асиметричного алгоритму шифрування є можливість перевірити, що користувач із приватним ключем – це користувач із публічним ключем. Це й буде гарантією того, що дані не були підроблені.

Користувач підписує транзакції за допомогою свого приватного ключа. Отже, є можливість перевірки «публічний ключ = підпис».

У разі невалідності транзакції (коли підпис і публічний ключ відправника не будуть збігатися) вона не буде розглядатися як об'єкт подальшого майнінгу.

Наприклад, у системі «Біткоїн» накопичуються транзакції. Далі ці транзакції валідуються майнерами. За успішної валідації всіх транзакцій формується новий блок, у якому зберігаються всі валідні транзакції, переводяться гроші з рахунку на рахунок, а майнер отримує нагороду.

Кожен блок у ланцюжку має обчислений хеш, а також хеш попереднього блоку (виняток стосується тільки першого блоку, в якому немає хешу попереднього блоку). За зміни будь-якого хешу відбудеться перерахунок хешу всіх наступних блоків, що буде говорити про те, що ланцюжок став не валідним. Саме ця особливість дає змогу будувати однорангові з'єднання між користувачами, які не можуть підробити інформацію про транзакції.

Висновки. Проведені дослідження показали, що технологія блокчейну активно розвивається й буде отримувати суттєві інвестиції. Частина галузей будуть революційним чином перебудовані; децентралізація змінить бізнес-логіку багатьох компаній та сервісів. За ступенем того, як ринок лібералізується, а ВДЕ зростає, технологія блокчейну пропонує спосіб, що дає змогу краще справлятися з усе більш складними та децентралізованими транзакціями між користувачами, великими й дрібними виробниками, промисловими підприємствами та навіть роздрібними торговцями й комунальними компаніями.

Фінансові додатки на основі технології блокчейну вже досягли високого рівня. Однак тільки час покаже, чи зможе ця технологія зробити революцію в енергетичному секторі. Перші пілотні проекти дають загальне уявлення про колосальні вигоди, які можуть забезпечити блокчейн-додатки щодо економії на витратах, а також швидкості та гнучкості. Україні необхідно активно включатися в цю сферу. Використання всіх видів технологій блокчейну, включаючи криптовалюту, має стати основою державної стратегії.

У сучасних умовах прийнята технологія обліку й контролю енергоресурсів не виправдовує себе. Причиною є організаційна й технічна недосконаліть структур, що здійснюють облік. Це стає причиною постійних збитків, тому автори статті розробили алгоритм системи обліку споживання та оплати платежів за енергоресурси. Надалі на підставі цього алгоритму буде створена сучасна автоматизована система.

Список літератури:

1. Nakamoto S. A Peer-to-Peer Electronic Cash System Bitcoin, 1–8. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 04.05.2019).

2. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. New York : Penguin Random House, 2016. 432 p.

3. Скворцов В. Блокчейн – не революция, это две инновации и одна потенциально успешная идея. URL: https://vc.ru/crypto/41715-blokcheyn-ne-revolyuciya-eto-dve-innovacii-i-odna-potencialno-uspeshnaya-ideya (дата звернення: 12.06.2019).

4. Deep Shift – Technology Tipping Points and Societal Impact (2015) / World Economic Forum Survey Report. URL: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_re-port_2015.pdf#page=24 (дата звернення: 10.05.2019).

5. Tar A. Smart Contracts, Explained. Cointelegraph. 2017. URL: https://cointelegraph.com/explained/smart-contracts-explained (дата звернення: 10.05.2019).

6. Segeda I. Blockchain as a digital economy promotion tool in energy Industry. *Modern Aspects of Software Development* : Proceedings of VI International Scientific and Practical Virtual Conference of Software Development Specialists, June, 24 2019. Kyiv : Igor Sikorsky KPI, 2019. P. 139–146.

7. Халезов А. Блокчейн и энергетика: 4 главных тренда. URL: https://medium.com/@khalezov/%D0%B1%D0%BB%D0%BE%D0%BA%D1%8 (дата звернення: 12.06.2019).

References:

1. Nakamoto S. (2009). Peer-to-Peer Electronic Cash System. *Bitcoin*, 1–8. Available at: https://bitcoin.org/en/bitcoin-paper (accessed: 04.05.2019).
2. Dan Tapscott & Alex Tapscott (2016). *Blockchain Revolution How the Technology Behind Bitcoin is Changing Money, Business, and the World*. New York : Penguin Random House. (in English)
3. Vadim Skvortsov (2018). Blokcheyn – ne revolyutsiya, eto dve innovatsii i odna potentsial'no uspeshnaya ideya [Blockchain is not a revolution, it is two innovations and one potentially successful idea]. Available at: https://vc.ru/crypto/41715-blokcheyn-ne-revolyuciya-eto-dve-innovacii-i-odna-potencialno-uspeshnaya-ideya) (accessed: 12.06.2019).
4. Deep Shift-Technology Tipping Points and Societal Impact (2015). *World Economic Forum Survey Report*. Available at: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_re-port_2015.pdf#page=24 (accessed: 10.05.2019).
5. Tar A. (2017). Smart Contracts, Explained. Cointelegraph. Available at: https://cointelegraph.com/explained/smart-contracts-explained (accessed: 10.05.2019).
6. Segeda I. (2019). Blockchain as a digital economy promotion tool in energy Industry. Modern Aspects of Software Development: Proceedings of *VI International Scientific and Practical Virtual Conference of Software Development Specialists (Ukrainian, Kyiv, June, 24, 2019 r.)*. Kyiv : Igor Sikorsky KPI, pp. 139–146.
7. Aleksey Khalezov (2018). Blokcheyn i energetika: 4 glavnykh trenda [Blockchain and energy: 4 main trends]. Available at: https://medium.com/@khalezov/%D0%B1%D0%BB%D0%BE%D0%BA%D1%8 (accessed: 04.08.2019).

РЕАЛИЗАЦИЯ ИСПОЛЬЗОВАНИЯ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В ЭНЕРГЕТИЧЕСКОМ СЕКТОРЕ

В статье проанализированы процессы вхождения криптовалют в энергетический сектор, вопросы преодоления определенной многозначности их виртуального и практического использования. Авторы концептуализируют этот процесс как цифровую блокчейн-революцию. Указано, что блокчейн является механизмом верификации транзакций в сети, повышает доверие клиентов и позволяет избавиться от посредников в финансовых операциях. Показаны потенциальные преимущества «умных контрактов», которые способны не только изменить технологический уклад, но и полностью поменять взаимоотношения субъектов общества, а также взаимоотношения между обществом и государством Рассмотрена децентрализованная модель энергетических транзакций и энергоснабжения. Представлены главные тренды блокчейна в энергетике. Предложен алгоритм системы учета потребления и оплаты платежей за энергоресурсы как блокчейн-приложение, которое будет реализовывать одноранговое взаимодействие между пользователями.

Ключевые слова: *криптовалюта, блокчейн, блокчейн-технологии, смарт-контракт, децентрализованная модель, энергетические транзакции.*

ACTUALIZATION OF BLOCKCHAIN-TECHNOLOGIES USE IN THE ENERGY SECTOR

Currently, blockchain technology is being developed as a stand-alone technology that can be applied outside of cryptocurrency systems. Blockchain and cryptocurrencies cannot be equated, to understand the essence of the matter, the authors consider features that are most clearly manifested when using blockchain technologies. The purpose of this study is to analyze the potential impact of blockchain technologies on the energy sector and explore the opportunities it may open to buyers and consumers of electricity. The paper analyzes the process of digital blockchain revolution and the impact of blockchain on the development of the economy's infrastructure. The functionality implemented in the process of the digital blockchain revolution may be a fully-fledged economic sphere that has not existed prior to the revolution. The modern concepts for the notions of cryptocurrency; blockchain; crypto assets given. In this paper options for using blockchain in the energy sector are presented. In particular, smart contracts allow you to interact with both: well-known and little-known partners, that is, they ensure trustful interaction between the parties automatically. The issue of assessing the complexity of transactions, a decentralized system of energy transactions and energy supply were examined in detail. Blockchain technology can provide the basis for creating a decentralized energy supply system. If conditions are created under which producers and consumers can interact directly, carrying out transactions directly in the network, electricity will become cheap. In this paper the main modern trends in the development of blockchain in the energy sector are considered. In today's world, the adopted technology of accounting and control of energy resources does not justify itself, and sometimes can be detrimental to the business entities using it. The paper presents an algorithm for a system of accounting for consumption and carrying out payments for energy resources on the basis of which an automated system will be developed. Blockchain technology is capable of fundamentally changing the energy system we are used to, first by transforming individual sectors, and ultimately by transforming the entire electricity market.

Key words: *cryptocurrency, blockchain, blockchain technology, smart contract, decentralized model, energy transactions.*